What is the difference between “consent” and “authorization” under the HIPAA Privacy Rule?

Answer:

The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. Covered entities that do so have complete discretion to design a process that best suits their needs.

By contrast, an “authorization” is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

# When is an authorization required from the patient before a provider or health plan engages in marketing to that individual?

### Answer:

The HIPAA Privacy Rule expressly requires an authorization for uses or disclosures of protected health information for ALL marketing communications, except in two circumstances:

1. When the communication occurs in a face-to-face encounter between the covered entity and the individual; or
2. The communication involves a promotional gift of nominal value.

If the marketing communication involves direct or indirect remuneration to the [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) from a third party, the authorization must state that such remuneration is involved.

# Will the HIPAA Privacy Rule hinder medical research by making doctors and others less willing and/or able to share with researchers information about individual patients?

### Answer:

We do not believe that the Privacy Rule will hinder medical research. Indeed, patients and health plan members should be more willing to authorize disclosures of their information for research and to participate in research when they know their information is protected. For example, in genetic studies conducted at the National Institutes of Health, nearly 32 percent of eligible people offered a test for breast cancer risk declined to take it. The overwhelming majority of those who refuse cite concerns about health insurance discrimination and loss of privacy as the reason. The Privacy Rule both permits important research and, at the same time, encourages patients to participate in research by providing much needed assurances about the privacy of their health information.

The Privacy Rule will require some covered health care providers and health plans to change their current practices related to documenting research uses and disclosures. It is possible that some covered health care providers and health plans may conclude that the Rule’s requirements for research uses and disclosures are too burdensome and will choose to limit researchers’ access to protected health information. We believe few providers will take this route, however, because the Common Rule includes similar, and more rigorous requirements, that have not impaired the willingness of researchers to undertake Federally-funded research. For example, unlike the Privacy Rule, the Common Rule requires an Institutional Review Board (IRB) review for all research proposals under its purview, even if informed consent is to be sought. The Privacy Rule requires documentation of IRB or Privacy Board approval only if patient authorization for the use or disclosure of protected health information for research purposes is to be altered or waived.

See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and fact review our [frequently asked questions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more information about the [Common Rule](https://www.hhs.gov/ohrp/humansubjects/commonrule/index.html?language=es)and Institutional Review and Privacy Boards.

# Are some of the criteria so subjective that inconsistent determinations may be made by Institutional Review Boards (IRB) and Privacy Boards reviewing similar or identical research projects?

### Answer:

Under the HIPAA Privacy Rule, Institutional Review Boards (IRBs) and Privacy Boards need to use their judgment as to whether the waiver criteria have been satisfied. Several of the waiver criteria are closely modeled on the Common Rule’s criteria for the waiver of informed consent and for the approval of a research study. Thus, it is anticipated that IRBs already have experience in making the necessarily subjective assessments of risks.

While IRBs or Privacy Boards may reach different determinations, the assessment of the waiver criteria through this deliberative process is a crucial element in the current system of safeguarding research participants’ privacy. The entire system of local IRBs is, in fact, predicated on a deliberative process that permits local IRB autonomy. The Privacy Rule builds upon this principle; it does not change it. Nonetheless, the Department will consider issuing guidance as necessary and appropriate to address concerns that may arise during implementation of these provisions.

See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and fact review our [frequently asked questions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more information about the Common Rule and Institutional Review and Privacy Boards.

# Does the HIPAA Privacy Rule prohibit researchers from conditioning participation in a clinical trial on an authorization to use/disclose existing protected health information?

### Answer:

No. The Privacy Rule does not address conditions for enrollment in a research study. Therefore, the Privacy Rule in no way prohibits researchers from conditioning enrollment in a research study on the execution of an authorization for the use of pre-existing health information.

# Does the HIPAA Privacy Rule permit the creation of a database for research purposes through an Institutional Review Board (IRB) or Privacy Board waiver of individual authorization?

### Answer:

Yes. A covered entity may use or disclose protected health information without individuals’ authorizations for the creation of a research database, provided the covered entity obtains documentation that an IRB or Privacy Board has determined that the specified waiver criteria were satisfied. Protected health information maintained by a covered entity in such a research database could be used or disclosed for future research studies as permitted by the Privacy Rule – that is, for future studies in which individual authorization has been obtained or where the Rule would permit research without an authorization, such as pursuant to an IRB or Privacy Board waiver.

See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and [frequently asked questions about the research provisions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more information about Institutional Review and Privacy Boards.

# How does the Rule help Institutional Review Boards (IRB) handle the additional responsibilities imposed by the HIPAA Privacy Rule?

### Answer:

Recognizing that some institutions may not have Institutional Review Boards (IRBs), or that some IRBs may not have the expertise needed to review research that requires consideration of risks to privacy, the Privacy Rule permits the [covered entity](http://edocket.access.gpo.gov/cfr_2002/octqtr/45cfr164.508.htm) to accept documentation of waiver of authorization from an alternative body called a Privacy Board–which could have fewer members, and members with different expertise than IRBs. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

In addition, the Rule allows an IRB to use expedited review procedures as permitted by the Common Rule to review and approve requests for waiver of authorizations. Similarly, the Rule permits Privacy Boards to use an expedited review process when the research involves no more than a minimal privacy risk to the individuals. An expedited review process permits covered entities to accept documentation of waiver of authorization when only one or more members of the IRB or Privacy Board have conducted the review.

See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and [frequently asked questions about the research provisions](https://www.hhs.gov/ocr/privacy/hipaa/faq/research_disclosures/index.html?language=es) for more information about the Common Rule.

# By establishing new waiver criteria and authorization requirements, hasn't the HIPAA Privacy Rule, in effect, modified the Common Rule?

### Answer:

No. Where both the Privacy Rule and the Common Rule apply, both regulations must be followed. The Privacy Rule regulates only the content and conditions of the documentation that [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) must obtain before using or disclosing protected health information for research purposes.

See our research section and frequently asked questions about the research provisions for more information about the Common Rule.

# Is documentation of Institutional Review Boards (IRB) and Privacy Board approval required by the HIPAA Privacy Rule before a covered entity would be permitted to disclose protected health information for research purposes without an individual's authorization?

### Answer:

No. The HIPAA Privacy Rule requires documentation of waiver approval by either an IRB or a Privacy Board, not both.

See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and [frequently asked questions about the research provisions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more information about Institutional Review and Privacy Boards.

# Does the HIPAA Privacy Rule require a covered entity to create an Institutional Review Board (IRB) or Privacy Board before using or disclosing protected health information for research?

### Answer:

No. The Institutional Review Board (IRB) or Privacy Board could be created by the [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) or the recipient researcher, or it could be an independent board.

See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and [frequently asked questions about the research provisions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more information about Institutional Review and Privacy Boards.

# What does the HIPAA Privacy Rule say about a research participant's right of access to research records or results?

### Answer:

With few exceptions, the Privacy Rule gives patients the right to inspect and obtain a copy of health information about themselves that is maintained by a [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) or its business associate in a “designated record set.” A designated record set is basically a group of records which a covered entity uses to make decisions about individuals, and includes a health care provider’s medical records and billing records, and a health plan’s enrollment, payment, claims adjudication, and case or medical management record systems. While it may be unlikely that a researcher would be maintaining a designated record set, any research records or results that are actually maintained by the covered entity as part of a designated record set would be accessible to research participants unless one of the Privacy Rule’s permitted exceptions applies.

One of the permitted exceptions applies to protected health information created or obtained by a covered health care provider/researcher for a clinical trial. The Privacy Rule permits the individual’s access rights in these cases to be suspended while the clinical trial is in progress, provided the research participant agreed to this denial of access when consenting to participate in the clinical trial. In addition, the health care provider/researcher must inform the research participant that the right to access protected health information will be reinstated at the conclusion of the clinical trial.

# Do the HIPAA Privacy Rule's requirements for authorization and the Common Rule's requirements for informed consent differ?

### Answer:

Yes. Under the Privacy Rule, a patient’s authorization is for the use and disclosure of protected health information for research purposes. In contrast, an individual’s informed consent, as required by the Common Rule and the Food and Drug Administration’s (FDA) human subjects regulations, is a consent to participate in the research study as a whole, not simply a consent for the research use or disclosure of protected health information. See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and [frequently asked questions about the research provisions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more informationabout the Common Rule.

For this reason, there are important differences between the Privacy Rule’s requirements for individual authorization, and the Common Rule’s and FDA’s requirements for informed consent. However, the Privacy Rule’s authorization elements are compatible with the Common Rule’s informed consent elements. Thus, both sets of requirements can be met by use of a single, combined form, which is permitted by the Privacy Rule.

For example, the Privacy Rule allows the research authorization to state that the authorization will be valid until the conclusion of the research study, or to state that the authorization will not have an expiration date or event. This is compatible with the Common Rule’s requirement for an explanation of the expected duration of the research subject’s participation in the study. It should be noted that where the Privacy Rule, the Common Rule, and/or FDA’s human subjects regulations are applicable, each of the applicable regulations will need to be followed.

# When is a researcher considered to be a covered health care provider under HIPAA?

### Answer:

A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. See [45 CFR 160.102, 160.103](http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr160_07.html).

For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the Privacy Rule. Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf. For further assistance in determining covered entity status, see the [CMS decision tool](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html).

# When does a covered entity have discretion to determine whether a research component of the entity is part of their covered functions, and therefore, subject to the HIPAA Privacy Rule?

### Answer:

A [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) that qualifies as a hybrid entity, meaning that the entity is a single legal entity that performs both covered and non-covered functions, may choose whether it wants to be a hybrid entity. If such a covered entity decides not to be a hybrid entity then it, and all of its components, are subject to the Privacy Rule in its entirety. Therefore, if a researcher is an employee or workforce member of a covered entity that has decided not to be a hybrid entity, the researcher is part of the covered entity and is, therefore, subject to the Privacy Rule.

If a covered entity decides to be a hybrid entity, it must define and designate its health care component(s). Research components of a hybrid entity that function as health care providers and engage in standard electronic transactions must be included in the hybrid entity's health care component(s), and be subject to the Privacy Rule.

However, research components that function as health care providers, but do not engage in standard electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, a hybrid entity, such as a university, has the option to include or exclude a research laboratory, that functions as a health care provider but does not engage in electronic transactions, as part of the hybrid entity’s health care component. If such a research laboratory is included in the hybrid entity’s health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity’s health care component, the employees or workforce members of the laboratory are not subject to the Privacy Rule.

# Can covered entities continue to disclose protected health information to the HHS Office for Human Research Protections for purposes of determining compliance with the HHS regulations for the protection of human subjects (45 CFR Part 46)?

### Answer:

Yes. The Office for Human Research Protections is a health oversight agency under the HIPAA Privacy Rule. Therefore, [covered entities](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) can continue to disclose protected health information to the Office for Human Research Protections for such compliance investigations either with patient authorization as provided at [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml), or without patient authorization for health oversight activities as permitted at [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(d).

# If a research subject revokes his or her authorization to have protected health information used or disclosed for research, does the HIPAA Privacy Rule permit a researcher/covered health care provider to continue using the protected health information already obtained prior to the time the individual revoked his or her authorization?

### Answer:

[Covered entities](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) may continue to use and disclose protected health information that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study. An individual may not revoke an authorization to the extent the covered entity has acted in reliance on the authorization. For research uses and disclosures, this reliance exception at [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml)(b)(5)(i) permits the continued use and disclosure of protected health information already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of the research study. For example, the reliance exception would permit the continued use and disclosure of protected health information to account for a subject’s withdrawal from the research study, as necessary to incorporate the information as part of a marketing application submitted to the Food and Drug Administration, to conduct investigations of scientific misconduct, or to report adverse events.

However, the reliance exception would not permit a covered entity to continue disclosing additional protected health information to a researcher or to use for its own research purposes information not already gathered at the time an individual withdraws his or her authorization.

# Can the preparatory research provision of the HIPAA Privacy Rule at 45 CFR 164.512(i)(1)(ii) be used to recruit individuals into a research study?

### Answer:

The preparatory research provision permits [covered entities](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity’s site. As such, a researcher who is an employee or a member of the covered entity’s workforce could use protected health information to contact prospective research subjects.

The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. In addition, the Rule permits a covered entity to disclose protected health information to the individual who is the subject of the information. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(a)(1)(i).

Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and without an Institutional Review Board (IRB) or Privacy Board waiver of the authorization. See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and [frequently asked questions about the research provisions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more information about Institutional Review and Privacy Boards.

However, a researcher who is not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of individual authorization by an IRB or Privacy Board as permitted at [45 CFR164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(i)(1)(i). The IRB or Privacy Board waiver of authorization permits the partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information as necessary to recruit potential research subjects. For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information as necessary for the researcher to be able to contact and recruit individuals into the study.

# Does the HIPAA Privacy Rule require documentation of Institutional Review Board (IRB) or Privacy Board approval of an alteration or waiver of individual authorization before a covered entity may use or disclose protected health information for any of the following provisions: (1) for preparatory research at 45 CFR 164.512(i)(1)(ii), (2)for research on the protected health information of decedents at 45 CFR 164.512(i)(1)(iii), or (3) a limited data set with a data use agreement as stipulated at 45 CFR 164.51?

### Answer:

No. Documentation of IRB or Privacy Board approval of an alteration or waiver of individual authorization is only needed before a covered entity may use or disclose protected health information under 45 CFR 164.512(i)(1)(i). See our [research section](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html?language=es) and [frequently asked questions about the research provisions](https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures?language=es) for more information about [Institutional Review](https://www.hhs.gov/ohrp/?language=es) and Privacy Boards.

# If research subjects' consent was obtained before the compliance date, but the Institutional Review Board (IRB) subsequently modifies the informed consent document after the compliance date and requires that subjects be reconsented, is authorization now required from these previously enrolled research subjects under the HIPAA Privacy Rule?

### Answer:

Yes. If informed consent or reconsent (ie., asked to sign a revised consent or another informed consent) is obtained from research subjects after the compliance date, the covered entity must obtain individual authorization as required at 45 CFR 164.508 for the use or disclosure of protected health information once the consent obtained before the compliance date is no longer valid for the research. The revised informed consent document may be combined with the authorization elements required by 45 CFR 164.508.

# May a covered entity use or disclose a patient’s entire medical record based on the patient’s signed authorization?

### Answer:

Yes, as long as the Authorization describes, among other things, the information to be used or disclosed by the [covered entity](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-530.xml) in a "specific and meaningful fashion," and is otherwise valid under the Privacy Rule. See [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml)(b)(1) and 164.508(c)(1)(i).

An Authorization would be valid if it authorized the covered entity to use or disclose an "entire medical record" or "complete patient file." On the other hand, without further definition, an Authorization to use or disclose "all protected health information" might not be sufficiently specific, since protected health information encompasses a wider range of information than that which is typically understood to be included in the medical record, and individuals are less likely to understand the breadth of information that may be defined as "protected health information."

# Does the Privacy Rule permit a covered entity to use or disclose protected health information pursuant to an authorization form that was prepared by a third party?

### Answer

Yes. A [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) is permitted to use or disclose protected health information pursuant to any Authorization that meets the Privacy Rule’s requirements at [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml). The Privacy Rule requires that an Authorization contain certain core elements and statements, but does not specify who may draft an Authorization (i.e., it could be drafted by any entity) or dictate any particular format for an Authorization. Thus, a covered entity may disclose protected health information as specified in a valid Authorization that has been created by another covered entity or a third party, such as an insurance company or researcher.

# May a valid authorization list categories of persons who may use or disclose protected health information, without naming specific individuals or entities?

### Answer:

Yes. One Authorization form may be used to authorize uses and disclosures by classes or categories of persons or entities, without naming the particular persons or entities. See [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml)(c)(1)(ii). For example, it would be sufficient if an Authorization authorized disclosures by "any health plan, physician, health care professional, hospital, clinic, laboratory, pharmacy, medical facility, or other health care provider that has provided payment, treatment or services to me or on my behalf" or if an Authorization authorized disclosures by "all medical sources." A separate Authorization specifically naming each health care provider from whom protected health information may be sought is not required.

Similarly, the Rule permits the identification of classes of persons to whom the [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) is authorized to make a disclosure. See [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml)(c)(1)(iii). Thus, a valid Authorization may authorize disclosures to a particular entity, particular person, or class of persons, such as "the employees of XYZ division of ABC insurance company."

# Can an individual revoke his or her authorization?

### Answer:

Yes. The Privacy Rule gives individuals the right to revoke, at any time, an Authorization they have given. The revocation must be in writing, and is not effective until the covered entity receives it. In addition, a written revocation is not effective with respect to actions a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) took in reliance on a valid Authorization, or where the Authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.

The Privacy Rule requires that the Authorization must clearly state the individual’s right to revoke; and the process for revocation must either be set forth clearly on the Authorization itself, or if the covered entity creates the Authorization, and its Notice of Privacy Practices contains a clear description of the revocation process, the Authorization can refer to the Notice of Privacy Practices. Authorization forms created by or submitted through a third party should not imply that revocation is effective when the third party receives it, since the revocation is not effective until a covered entity which had previously been authorized to make the disclosure receives it.

# Is a copy, facsimile, or electronically transmitted version of a signed authorization valid under the Privacy Rule?

### Answer:

Yes. Under the Privacy Rule, a covered entity may use or disclose protected health information pursuant to a copy of a valid and signed Authorization, including a copy that is received by facsimile or electronically transmitted.

# Must an authorization include an expiration date?

### Answer:

The Privacy Rule requires that an Authorization contain either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For example, an Authorization may expire "one year from the date the Authorization is signed," "upon the minor’s age of majority," or "upon termination of enrollment in the health plan."

An Authorization remains valid until its expiration date or event, unless effectively revoked in writing by the individual before that date or event. The fact that the expiration date on an Authorization may exceed a time period established by State law does not invalidate the Authorization under the Privacy Rule, but a more restrictive State law would control how long the Authorization is effective.

# May a covered entity disclose protected health information specified in an authorization, even if that information was created after the authorization was signed?

### Answer:

Yes, provided that the Authorization encompasses the category of information that was later created, and that the Authorization has not expired or been revoked by the individual. Unless otherwise expressly limited by the Authorization, a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may use or disclose the protected health information identified on the Authorization regardless of when the information was created.

# Does the Privacy Rule require that an authorization be notarized or include a witness signature?

### Answer:

The Privacy Rule does not require that a document be notarized or witnessed.

# Can an authorization be used together with other written instructions from the intended recipient of the information?

### Answer:

A transmittal or cover letter can be used to narrow or provide specifics about a request for protected health information as described in an Authorization, but it cannot expand the scope of the Authorization.

For example, if an individual has authorized the disclosure of "all medical records" to an insurance company, the insurance company could by cover letter narrow the request to the medical records for the last 12 months. The cover letter could also specify a particular employee or address for the "class of persons" designated in the Authorization to receive the information. By contrast, an insurance company could not by cover letter extend the expiration date of an Authorization, or expand the scope of information set forth in the Authorization.

# Does the HIPAA Privacy Rule permit doctors, nurses, and other health care providers to share patient health information for treatment purposes without the patient’s authorization?

### Answer:

Yes. The Privacy Rule allows those doctors, nurses, hospitals, laboratory technicians, and other health care providers that are covered entities to use or disclose protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient’s authorization. This includes sharing the information to consult with other providers, including providers who are not covered entities, to treat a different patient, or to refer the patient. See [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml).

# What were the major modifications to the HIPAA Privacy Rule that the Department of Health and Human Services (HHS) adopted in August 2002?

### Answer:

Based on the information received through public comments, testimony at public hearings, meetings at the request of industry and other stakeholders, as well as other communications, HHS identified a number of areas in which the Privacy Rule, as issued in December 2000, would have had potential unintended effects on health care quality or access. As a result, HHS proposed modifications that would maintain strong protections for the privacy of individually identifiable health information, address the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieve unintended administrative burdens created by the Privacy Rule.

Final modifications to the Rule were adopted on August 14, 2002. Among other things, the modifications addressed the following aspects of the Privacy Rule:

* Uses and disclosures for treatment, payment and health care operations, including eliminating the requirement for the individual’s consent for these activities;
* The notice of privacy practices that [covered entities](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) must provide to patients;
* Uses and disclosures for marketing purposes;
* Minimum necessary uses and disclosures;
* Parents as the personal representatives of unemancipated minors;
* Uses and disclosures for research purposes; and
* Transition provisions, including business associate contracts.

In addition to these key areas, the modifications included changes to certain other provisions where necessary to clarify the Privacy Rule, and a list of technical corrections intended as editorial or typographical corrections to the Privacy Rule.

# Can a CSP be considered to be a “conduit” like the postal service, and, therefore, not a business associate that must comply with the HIPAA Rules?

### Answer:

Generally, no. CSPs that provide cloud services to a covered entity or business associate that involve creating, receiving, or maintaining (e.g., to process and/or store) electronic protected health information (ePHI) meet the definition of a business associate, even if the CSP cannot view the ePHI because it is encrypted and the CSP does not have the decryption key.

As explained in previous guidance,[[i]](https://www.hhs.gov/hipaa/for-professionals/faq/2077/can-a-csp-be-considered-to-be-a-conduit-like-the-postal-service-and-therefore-not-a-business%20associate-that-must-comply-with-the-hipaa-rules/index.html%22%20%5Cl%20%22_edn1%22%20%5Co%20%22) the conduit exception is limited to transmission-only services for PHI (whether in electronic or paper form), including any temporary storage of PHI incident to such transmission. Any access to PHI by a conduit is only transient in nature. In contrast, a CSP that maintains ePHI for the purpose of storing it will qualify as a business associate, and not a conduit, even if the CSP does not actually view the information, because the entity has more persistent access to the ePHI.

Further, where a CSP provides transmission services for a covered entity or business associate customer, in addition to maintaining ePHI for purposes of processing and/or storing the information, the CSP is still a business associate with respect to such transmission of ePHI.  The conduit exception applies where the only services provided to a covered entity or business associate customer are for transmission of ePHI that do not involve any storage of the information other than on a temporary basis incident to the transmission service.

# Which CSPs offer HIPAA-compliant cloud services?

### Answer:

OCR does not endorse, certify, or recommend specific technology or products.

# What if a HIPAA covered entity (or business associate) uses a CSP to maintain ePHI without first executing a business associate agreement with that CSP?

### Answer:

If a covered entity (or business associate) uses a CSP to maintain (e.g., to process or store) electronic protected health information (ePHI) without entering into a BAA with the CSP, the covered entity (or business associate) is in violation of the HIPAA Rules.  45 C.F.R §§164.308(b)(1) and §164.502(e).  OCR has entered into a resolution agreement and corrective action plan with a covered entity that OCR determined stored ePHI of over 3,000 individuals on a cloud-based server without entering into a BAA with the CSP.[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2079/what-if-a-hipaa-covered-entity-or-business-associate-uses-a-csp-to-maintain-ephi-without-first-executing-a-business-associate-agreement-with-that-csp/index.html%22%20%5Cl%20%22_ftn1%22%20%5Co%20%22)

Further, a CSP that meets the definition of a business associate – that is a CSP that creates, receives, maintains, or transmits PHI on behalf of a covered entity or another business associate – must comply with all applicable provisions of the HIPAA Rules, regardless of whether it has executed a BAA with the entity using its services. See 78 Fed. Reg. 5565, 5598 (January 25, 2013).  OCR recognizes that there may, however, be circumstances where a CSP may not have actual or constructive knowledge that a covered entity or another business associate is using its services to create, receive, maintain, or transmit ePHI.   The HIPAA Rules provide an affirmative defense in cases where a CSP takes action to correct any non-compliance within 30 days (or such additional period as OCR may determine appropriate based on the nature and extent of the non-compliance) of the time that it knew or should have known of the violation (e.g., at the point the CSP knows or should have known that a covered entity or business associate customer is maintaining ePHI in its cloud).  45 CFR 160.410.  This affirmative defense does not, however, apply in cases where the CSP was not aware of the violation due to its own willful neglect.

If a CSP becomes aware that it is maintaining ePHI, it must come into compliance with the HIPAA Rules, or securely return the ePHI to the customer or, if agreed to by the customer, securely destroy the ePHI.  Once the CSP securely returns or destroys the ePHI (subject to arrangement with the customer), it is no longer a business associate.  We recommend CSPs document these actions.

While a CSP maintains ePHI, the HIPAA Rules prohibit the CSP from using or disclosing the data in a manner that is inconsistent with the Rules.

# If a CSP experiences a security incident involving a HIPAA covered entity’s or business associate’s ePHI, must it report the incident to the covered entity or business associate?

### Answer:

Yes.    The Security Rule at 45 CFR § 164.308(a)(6)(ii) requires business associates to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate; and document security incidents and their outcomes.  In addition, the Security Rule at 45 CFR § 164.314(a)(2)(i)(C) provides that a business associate agreement must require the business associate to report, to the covered entity or business associate whose electronic protected health information (ePHI) it maintains, any security incidents of which it becomes aware.  A security incident under 45 CFR § 164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.  Thus, a business associate CSP must implement policies and procedures to address and document security incidents, and must report security incidents to its covered entity or business associate customer.

The Security Rule, however, is flexible and does not prescribe the level of detail, frequency, or format of reports of security incidents, which may be worked out between the parties to the business associate agreement (BAA).  For example, the BAA may prescribe differing levels of detail, frequency, and formatting of reports based on the nature of the security incidents – e.g., based on the level of threat or exploitation of vulnerabilities, and the risk to the ePHI they pose.  The BAA could also specify appropriate responses to certain incidents and whether identifying patterns of attempted security incidents is reasonable and appropriate.

Note, though, that the Breach Notification Rule specifies the content, timing, and other requirements for a business associate to report incidents that rise to the level of a breach of unsecured PHI to the covered entity (or business associate) on whose behalf the business associate is maintaining the PHI.  See 45 CFR § 164.410. The BAA may specify more stringent (e.g., more timely) requirements for reporting than those required by the Breach Notification Rule (so long as they still also meet the Rule’s requirements) but may not otherwise override the Rule’s requirements for notification of breaches of unsecured PHI.

# Do the HIPAA Rules allow health care providers to use mobile devices to access ePHI in a cloud?

### Answer:

Yes.  Health care providers, other covered entities, and business associates may use mobile devices to access electronic protected health information (ePHI) in a cloud as long as appropriate physical, administrative, and technical safeguards are in place to protect the confidentiality, integrity, and availability of the ePHI on the mobile device and in the cloud, and appropriate BAAs are in place with any third party service providers for the device and/or the cloud that will have access to the e-PHI.   The HIPAA Rules do not endorse or require specific types of technology, but rather establish the standards for how covered entities and business associates may use or disclose ePHI through certain technology while protecting the security of the ePHI by requiring analysis of the risks to the ePHI posed by such technology and implementation of reasonable and appropriate administrative, technical, and physical safeguards to address such risks.  OCR and ONC have issued guidance on the use of [mobile devices and tips](https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device) for securing ePHI on mobile devices.[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2081/do-the-hipaa-rules-allow-health-care-providers-to-use-mobile-devices-to-access-ephi-in-a-cloud/index.html#_ftn1)

# Do the HIPAA Rules require a CSP to maintain ePHI for some period of time beyond when it has finished providing services to a covered entity or business associate?

### Answer:

No, the HIPAA Rules generally do not require a business associate to maintain electronic protected health information (ePHI) beyond the time it provides services to a covered entity or business associate.  The Privacy Rule provides that a business associate agreement (BAA) must require a business associate to return or destroy all PHI at the termination of the BAA where feasible.  45 CFR  § 164.504(e)(2)(J).

If such return or destruction is not feasible, the BAA must extend the privacy and security protections of the BAA to the ePHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.  For example, return or destruction would be considered ‘‘infeasible’’ if other law requires the business associate CSP to retain ePHI for a period of time beyond the termination of the business associate contract.[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2082/do-the-hipaa-rules-require-a-csp-to-maintain-ephi-for-some-period-of-time-beyond-when-it-has-finished-providing-services-to-a-covered-entity-or-business-associate/index.html#_ftn1)

# Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside of the United States?

### Answer:

Yes, provided the covered entity (or business associate) enters into a business associate agreement (BAA) with the CSP and otherwise complies with the applicable requirements of the HIPAA Rules. However, while the HIPAA Rules do not include requirements specific to protection of electronic protected health information (ePHI) processed or stored by a CSP or any other business associate outside of the United States, OCR notes that the risks to such ePHI may vary greatly depending on its geographic location. In particular, outsourcing storage or other services for ePHI overseas may increase the risks and vulnerabilities to the information or present special considerations with respect to enforceability of privacy and security protections over the data. Covered entities (and business associates, including the CSP) should take these risks into account when conducting the risk analysis and risk management required by the Security Rule. See 45 CFR §§ 164.308(a)(1)(ii)(A) and (a)(1)(ii)(B). For example, if ePHI is maintained in a country where there are documented increased attempts at hacking or other malware attacks, such risks should be considered, and entities must implement reasonable and appropriate technical safeguards to address such threats.

# Do the HIPAA Rules require CSPs that are business associates to provide documentation, or allow auditing, of their security practices by their customers who are covered entities or business associates?

### Answer:

No. The HIPAA Rules require covered entity and business associate customers to obtain satisfactory assurances in the form of a business associate agreement (BAA) with the CSP that the CSP will, among other things, appropriately safeguard the protected health information (PHI) that it creates, receives, maintains or transmits for the covered entity or business associate in accordance with the HIPAA Rules.  The CSP is also directly liable for failing to safeguard electronic PHI in accordance with the Security Rule[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2084/do-the-hipaa-rules-require-csps-that-are-business-associates-to-provide-documentation-or-allow-auditing-of-their-security-practices-by-their-customers-who-are-covered-entities-or-business-associates/index.html#_ftn1) and for impermissible uses or disclosures of the PHI.[[2]](https://www.hhs.gov/hipaa/for-professionals/faq/2084/do-the-hipaa-rules-require-csps-that-are-business-associates-to-provide-documentation-or-allow-auditing-of-their-security-practices-by-their-customers-who-are-covered-entities-or-business-associates/index.html%22%20%5Cl%20%22_ftn2%22%20%5Co%20%22)  The HIPAA Rules do not expressly require that a CSP provide documentation of its security practices to or otherwise allow a customer to audit its security practices.   However, customers may require from a CSP (through the BAA, service level agreement, or other documentation) additional assurances of protections for the PHI, such as documentation of safeguards or audits, based on their own risk analysis and risk management or other compliance activities.

# If a CSP receives and maintains only information that has been de-identified in accordance with the HIPAA Privacy Rule, is it is a business associate?

### Answer:

No. A CSP is not a business associate if it receives and maintains (e.g., to process and/or store) only information de-identified following the processes required by the Privacy Rule.  The Privacy Rule does not restrict the use or disclosure of de-identified information, nor does the Security Rule require that safeguards be applied to de-identified information, as the information is not considered protected health information. See the [OCR guidance on de-identification](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html) for more information.[[1]](https://www.hhs.gov/hipaa/for-professionals/faq/2085/if-a-csp-receives-and-maintains-only-information-that-has-been-de-identified-in-accordance-with-the-hipaa-privacy-rule-is-it-is-a-business-associate/index.html#_ftn1)

# Has the Secretary exceeded the HIPAA statutory authority by requiring "satisfactory assurances" for disclosures to business associates?

### Answer:

No. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gives the Secretary authority to directly regulate health plans, health care clearinghouses, and certain health care providers. It also grants the Department explicit authority to regulate the uses and disclosures of protected health information maintained and transmitted by [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html). Therefore, the Department does have the authority to condition the disclosure of protected health information by a covered entity to a business associate on the covered entity’s having a written contract with that business associate.

# Were there Privacy Rule compliance deadlines in 2004?

### Answer:

By April 14, 2004:

* "Small health plans" (health plans with annual receipts of $5 million or less), must be in compliance with the Privacy Rule; and
* [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) (including small health plans) had to have in place with their business associates written contracts or arrangements that meet Privacy Rule requirements.

Small Health Plans. Small health plans that are subject to HIPAA received an additional year – until April 14, 2004 – to come into compliance with the Privacy Rule. See [45 CFR 164.534(b)(2)](https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR).

Plans that are self-administered and have fewer than 50 participants are excluded from HIPAA’s Administrative Simplification requirements. (See the Answer to the FAQ "[Must all small health plans comply with the Privacy Rule?](https://www.hhs.gov/ocr/privacy/hipaa/faq/smaller_providers_and_businesses/495.html)") The Department of Health and Human Services’ (HHS) "[Are you a Covered Entity?](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)" decision tool helps entities determine whether they are health plans or other HIPAA covered entities. These materials, hundreds of FAQs, and a wide range of other guidance and materials to assist covered entities in complying with HIPAA and the Privacy Rule, are available on the OCR Web site.

Business Associate Agreements. As of April 14, 2004, whenever the Privacy Rule requires covered entities to have written contracts or other arrangements with their business associates, these documents must include provisions that comply with Privacy Rule requirements. As modified in August, 2002, the Privacy Rule provided most covered entities with up to one additional year – or until April 14, 2004 – to amend written contracts or other written arrangements that existed prior to October 15, 2002, to meet the Rule’s business associate requirements. (Unless they renewed automatically, contracts or other written arrangements were not eligible for this transition period if they were renewed, modified or newly entered into on or after October 15, 2002.) See 45 CFR 164.532(d) and (e). To assist covered entities in meeting these requirements, OCR has published a Fact Sheet regarding compliance with the Privacy Rule’s business associate requirements, sample business associate contract provisions, and a number of related Answers to Frequently Asked Questions, all of which are available on the [OCR Privacy Web site](https://www.hhs.gov/ocr/privacy/).

# Is a covered entity liable for, or required to monitor, the actions of its business associates?

### Answer:

No. The HIPAA Privacy Rule requires [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See [45 CFR 164.504](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml)(e)(1).

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of protected health information to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity.

# May a covered entity share protected health information directly with another covered entity's business associate?

### Answer:

Yes. If the HIPAA Privacy Rule permits a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to share protected health information with another covered entity, the covered entity is permitted to make the disclosure directly to a business associate acting on behalf of that other covered entity.

# When may a covered health care provider disclose protected health information, without an authorization or business associate agreement, to a medical device company representative?

### Answer:

In general, and as explained below, the Privacy Rule permits a covered health care provider (covered provider), without the individual’s written authorization, to disclose protected health information to a medical device company representative (medical device company) for the covered provider’s own treatment, payment, or health care operation purposes ([45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml)(c)(1)), or for the treatment or payment purposes of a medical device company that is also a health care provider (45 CFR 164.506(c)(2), (3)). Additionally, the public health provisions of the Privacy Rule permit a covered provider to make disclosures, without an authorization, to a medical device company or other person that is subject to the jurisdiction of the Food and Drug Administration (FDA) for activities related to the quality, safety, or effectiveness of an FDA-regulated product or activity for which the person has responsibility. See [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(b)(1)(iii) and the frequently asked questions on public health disclosures for more information.

In certain situations, a covered health care provider may disclose protected health information to a medical device company without an individual’s written authorization only if the medical device company is a health care provider as defined by the Rule. A medical device company meets the Privacy Rule’s definition of “health care provider” if it furnishes, bills, or is paid for “health care” in the normal course of business. “Health care” under the Rule means care, services or supplies related to the health of an individual. Thus, a device manufacturer is a health care provider under the Privacy Rule if it needs protected health information to counsel a surgeon on or determine the appropriate size or type of prosthesis for the surgeon to use during a patient’s surgery, or otherwise assists the doctor in adjusting a device for a particular patient. Similarly, when a device company needs protected health information to provide support and guidance to a patient, or to a doctor with respect to a particular patient, regarding the proper use or insertion of the device, it is providing “health care” and, therefore, is a health care provider when engaged in these services. See 65 FR 82569. By contrast, a medical device company is not providing “health care” if it simply sells its appropriately labeled products to another entity for that entity to use or dispense to individuals.

The following are some examples of circumstances in which a covered provider may share protected health information with a medical device company, without the individual’s authorization:

* A covered provider may disclose protected health information needed for an orthopaedic device manufacturer or its representative to determine and deliver the appropriate range of sizes of a prosthesis for the surgeon to use during a particular patient’s surgery. (This would be a treatment disclosure to the device company as a health care provider. Exchanges of protected health information between health care providers for treatment of the individual are not subject to the minimum necessary standards. [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(b).)
* The device manufacturer or its representative may be present in the operating room, as requested by the surgeon, to provide support and guidance regarding the appropriate use, implantation, calibration or adjustment of a medical device for that particular patient. (This would be treatment by the device company as a health care provider. As noted in the prior example, treatment disclosures between health care providers are not subject to the minimum necessary standards.)
* A covered provider may allow a representative of a medical device manufacturer to view protected health information, such as films or patient records, to provide consultation, advice or assistance where the provider, in her professional judgment, believes that this will assist with a particular patient’s treatment. (This would also be a treatment disclosure and minimum necessary would not apply.)
* A covered provider may share protected health information with a medical device company as necessary for the device company to receive payment for the health care it provides. (This would be a disclosure for payment of a health care provider and subject to minimum necessary standards.)
* A covered provider may disclose protected health information to a medical device manufacturer that is subject to FDA jurisdiction to report an adverse event, to track an FDA-regulated product, or other purposes related to the quality, safety, or effectiveness of the FDA-regulated product. (This would be a public health disclosure and subject to minimum necessary standards.)

A business associate agreement would not usually be required for the disclosures noted above. For example, a business associate agreement would not be needed for disclosures between health care providers for the treatment of the individual ([45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(e)(1)(ii)(A)). Likewise, a medical device company would not be a business associate of a covered provider with respect to public health disclosures to a device company that is subject to FDA jurisdiction or disclosures to a device company as a health care provider for that company’s payment purposes, as in neither case is the device company performing a function or activity on behalf of, nor providing a specified service to, the covered provider. See 45 CFR 160.103. In other circumstances, however, a business associate agreement may be required even if the disclosure were permitted without an authorization. For example, a business associate agreement would be required if a covered entity asked the medical device company to provide an estimate of the cost savings it might expect from the use of a particular medical device; and to do so, the device company needed access to the covered entity’s protected health information. In this case, the medical device company is performing a health care operations function (business planning and development) on behalf of the covered provider, which requires a business associate agreement even though the disclosure is permitted without an authorization.

# Must a covered health care provider obtain an individual’s authorization to use or disclose protected health information to an interpreter?

### Answer:

No, when a covered health care provider uses an interpreter to communicate with an individual, the individual’s authorization is not required when the provider meets the conditions below. Covered entities may use and disclose protected health information for treatment, payment and health care operations without an individual’s authorization, [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml)(c). A covered health care provider might use interpreter services to communicate with patients who speak a language other than English or who are deaf or hard of hearing, and provision of interpreter services usually will be a health care operations function of the covered entity as defined at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml).

When using interpreter services, a covered entity may use and disclose protected health information regarding an individual without an individual’s authorization as a health care operation, in accordance with the Privacy Rule, in the following ways:

* When the interpreter is a member of the covered entity’s workforce (i.e., a bilingual employee, a contract interpreter on staff, or a volunteer) as defined at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml);
* When a covered entity engages the services of a person or entity, who is not a workforce member, to perform interpreter services on its behalf, as a business associate, as defined at 45 CFR 160.103. A covered entity may disclose protected health information as necessary for the business associate to provide interpreter services on the covered entity’s behalf, subject to certain written satisfactory assurances set forth in [45 CFR 164.504](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml)(e). For instance, many providers including those that are recipients of federal financial assistance and are required under Title VI of the Civil Rights Act of 1964 to take reasonable steps to provide meaningful access to persons with limited English proficiency -- will have contractual arrangements with private commercial companies, community-based organizations, or telephone interpreter service lines to provide such language services. If a covered entity has an ongoing contractual relationship with an interpreter service, that service arrangement should comply with the Privacy Rule business associate agreement requirements.

In addition, a covered health care provider may, without the individual’s authorization, use or disclose protected health information to the patient’s family member, close friend, or any other person identified by the individual as his or her interpreter for a particular healthcare encounter. In these situations, that interpreter is not a business associate of the health care provider. As with other disclosures to family members, friends or other persons identified by an individual as involved in his or her care, when the individual is present, the covered entity may obtain the individual’s agreement or reasonably infer, based on the exercise of professional judgment, that the individual does not object to the disclosure of protected health information to the interpreter. [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b)(2).

For example, if a covered health care provider encounters a patient who speaks a language for which the provider has no employee, volunteer member of the workforce or contractor who can competently interpret, but then is able to identify a telephone interpreter service to communicate with the patient, the provider may contact the telephone interpreter service and identify the language used by the patient, so that the interpreter may explain to the patient that the interpreter is available to assist the patient in communicating with the provider. If the provider reasonably concludes that the patient has chosen to be assisted by the interpreter, and, by the patient’s willingness to continue the health care encounter using the interpreter, reasonably infers that the individual does not object to the disclosure, protected health information may be disclosed in accordance with [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b) without a business associate contract.

Organizations that are subject to both HIPAA and Title VI must comply with the requirements of both laws, though not all HIPAA covered entities are recipients of federal financial assistance and thus, required to comply with Title VI; and not all recipients of federal financial assistance are also HIPAA covered entities, subject to the Privacy Rule. For information about the obligation of recipients of federal financial assistance to take reasonable steps to provide meaningful access to persons who are limited English proficient, see [Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons](https://www.hhs.gov/ocr/civilrights/resources/specialtopics/lep/factsheetguidanceforlep.html). This guidance includes information for recipients of federal financial assistance about important considerations for determining the competency of interpreters, such as their understanding of applicable confidentiality requirements, that should be taken into account when using interpreters arranged by the provider or when individuals elect to use friends, family or others as interpreters. HIPAA covered entities may also be required to comply with the Americans with Disabilities Act and/or Section 504 of the Rehabilitation Act of 1973, both of which have requirements for the provision of sign language and oral interpreters for people who are deaf or hard of hearing. See our [frequently asked question on the use of communications assistants as part of a Telecommunications Relay Service (TRS)](https://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/500.html).

# Can health care providers invite or arrange for members of the media, including film crews, to enter treatment areas of their facilities without prior written authorization?

### Answer:

**Health care providers cannot invite or allow media personnel, including film crews, into treatment or other areas of their facilities where patients’ PHI will be accessible in written, electronic, oral, or other visual or audio form, or otherwise make PHI accessible to the media, without prior written authorization from each individual who is or will be in the area or whose PHI otherwise will be accessible to the media.  Only in very limited circumstances, as set forth below, does the HIPAA Privacy Rule permit health care providers to disclose protected health information to members of the media without a prior authorization signed by the individual.**

A covered entity, including a health care provider, may not use or disclose protected health information (PHI), except either: (1) as the HIPAA Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing. Generally, the HIPAA Privacy Rule does not permit health care providers to disclose PHI to media personnel, including film crews, without having previously obtained a HIPAA-compliant authorization signed by the patient or his or her personal representative. In other words, health care providers may not allow members of the media, including film crews, into treatment areas of their facilities or other areas where PHI will be accessible in written, electronic, oral or other visual or audio form, without prior authorization from the patients who are or will be in the area or whose PHI will be accessible to the media.  It is not sufficient for a health care provider to request or require media personnel to mask the identities of patients (using techniques such as blurring, pixelation, or voice alteration software) for whom an authorization was not obtained, because the HIPAA Privacy Rule does not allow media access to the patients’ PHI, absent an authorization, in the first place.

In addition, the health care provider must ensure that reasonable safeguards are in place to protect against impermissible disclosures or to limit incidental disclosures of other PHI that may be in the area but for which an authorization has not been obtained.

There are very limited situations in which the HIPAA Privacy Rule permits a covered entity to disclose limited PHI to the media without obtaining a HIPAA authorization.  For example, a covered entity may seek to have the media help identify or locate the family of an unidentified and incapacitated patient in its care.  In that case, the covered entity may disclose limited PHI about the incapacitated patient to the media if, in the hospital’s professional judgment, doing so is in the patient’s best interest.  See 45 C.F.R. 164.510(b)(1)(ii).  In addition, a covered entity may disclose a patient’s location in the facility and condition in general terms that do not communicate specific medical information about the individual to any person, including the media, without obtaining a HIPAA authorization where the individual has not objected to his information being included in the facility directory, and the media representative or other person asks for the individual by name.  See 45 C.F.R. 164.510(a).

The HIPAA Privacy Rule does not require health care providers to prevent members of the media from entering areas of their facilities that are otherwise generally accessible to the public, which may include public waiting areas or areas where the public enters or exits the facility.

A health care provider may utilize the services of a contract film crew to produce training videos or public relations materials on the provider’s behalf if certain protections are in place.  If patients are to be identified by the provider and interviewed by a film crew, or if PHI might be accessible during filming or otherwise disclosed, the provider must enter into a HIPAA business associate agreement with the film crew acting as a business associate.  Among other requirements, the business associate agreement must ensure that the film crew will safeguard the PHI it obtains, only use or disclose the PHI for the purposes provided in the agreement, and return or destroy any PHI after the work for the health care provider has been completed.  See 45 C.F.R. 164.504(e)(2).  As a business associate, the film crew must comply with the HIPAA Security Rule and a number of provisions in the Privacy Rule, including the Rule’s restrictions on the use and disclosure of PHI.  In addition, authorizations from patients whose PHI is included in any materials would be required before such materials are posted online, printed in brochures for the public, or otherwise publicly disseminated.

Finally, covered entities can continue to inform the media of their treatment services and programs so that the media can better inform the public, provided that, in doing so, the covered entity does not share PHI with the media without the prior authorization of the individuals who are the subject of the PHI.

# Instead of entering into a contract, can business associates self-certify or be certified by a third party as compliant with the HIPAA Privacy Rule?

### Answer:

No. A covered entity is required to enter into a contract or other written arrangement with a business associate that meets the requirements at [45 CFR 164.504](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml)(e).

# Is a business associate contract required for a covered entity to disclose protected health information to a researcher?

### Answer:

No. Disclosures from a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to a researcher for research purposes do not require a business associate contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity’s own behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of “business associate” at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml).

However, the HIPAA Privacy Rule does not prohibit a covered entity from entering into a business associate contract with a researcher if the covered entity wishes to do so. Notwithstanding the above, a covered entity is only permitted to disclose protected health information to a researcher as permitted by Rule, that is, with an individual’s authorization pursuant to [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml), without an individual’s authorization as permitted by [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(i), or as a limited data set provided that a data use agreement is in place as permitted by [45 CFR 164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(e).

# Are covered entities that engage in joint activities under an organized health care arrangement (OHCA) required to have business associate contracts with each other?

### Answer:

No. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) that participate in an OHCA are permitted to share protected health information for the joint health care activities of the OHCA without entering into business associate contracts with each other. Of course, each such entity is independently required to observe its obligations under the HIPAA Privacy Rule with respect to protected health information.

# Is a business associate contract required with organizations or persons where inadvertent contact with protected health information may result - such as in the case of janitorial services?

### Answer:

A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. Generally, janitorial services that clean the offices or facilities of a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) are not business associates because the work they perform for covered entities does not involve the use or disclosure of protected health information, and any disclosure of protected health information to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the HIPAA Privacy Rule. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(a)(1).

If a service is hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity’s premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service.

# Is a physician required to have business associate contracts with technicians such as plumbers, electricians or photocopy machine repairmen who provide repair services in a physician's office?

### Answer:

No, plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician’s office, so they do not meet the definition of a “business associate”. Under the HIPAA Privacy Rule, “business associates” are contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information. See the definition of “business associate” at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml).

Any disclosure of protected health information to such technicians that occurs in the performance of their duties (such as may occur walking through or working in file rooms) is limited in nature, occurs as a by-product of their duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the Privacy Rule. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(a)(1).

# Would business associate contracts in electronic form, with an electronic signature, satisfy the HIPAA Privacy Rule's business associate contract requirements?

### Answer:

Yes, assuming that the electronic contract satisfies the applicable requirements of State contract law. The Privacy Rule generally allows for electronic documents, including business associate contracts, to qualify as written documents for purposes of meeting the Rule’s requirements.

However, currently, no standards exist under HIPAA for electronic signatures. In the absence of specific standards, [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) must ensure any electronic signature used will result in a legally binding contract under applicable State or other law.

# Do physicians with hospital privileges have to enter into business associate contracts with the hospital?

### Answer:

No. The hospital and such physicians participate in what the HIPAA Privacy Rule defines as an organized health care arrangement (OHCA). Thus, they may use and disclose protected health information for the joint health care activities of the OHCA without entering into a business associate agreement.

# Are accreditation organizations business associates of the covered entities they accredit?

### Answer:

Yes. The HIPAA Privacy Rule explicitly defines organizations that accredit [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) as business associates. See the definition of “business associate” at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml).

Like other business associates, accreditation organizations provide a service to the covered entity which requires the sharing of protected health information. The business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity. As an alternative to the business associate contract, covered entities may disclose a limited data set of protected health information, not including direct identifiers, to an accreditation organization, subject to a data use agreement. See [45 CFR 164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(e).

If only a limited data set of protected health information is disclosed, the satisfactory assurances required of the business associate are satisfied by the data use agreement.

# When is a health care provider a business associate of another health care provider?

### Answer:

The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to a health care provider for treatment purposes. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(e)(1).

Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose.
For example, a hospital may enlist the services of another health care provider to assist in the hospital’s training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.

# Are the following entities considered "business associates" under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

### Answer:

No, the Privacy Rule does not require a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.

# If the only protected health information a business associate receives is a limited data set, does the HIPAA Privacy Rule require the covered entity to enter into both a business associate agreement and data use agreement with the business associate?

### Answer:

No. Where a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) discloses only a limited data set to a business associate for the business associate to carry out a health care operations function, the covered entity satisfies the Rule’s requirements that it obtain satisfactory assurances from its business associate with the data use agreement.

For example, where a State hospital association receives only limited data sets of protected health information from its member hospitals for the purposes of conducting and sharing comparative quality analyses with these hospitals, the member hospitals need only have data use agreements in place with the State hospital association.

# Are business associates required to restrict their uses and disclosures to the minimum necessary? May a covered entity reasonably rely on a request from a covered entity's business associate as the minimum necessary?

### Answer:

A [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)’s contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See [45 CFR 164.504](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml)(e)(2)(i). Thus, a business associate contract must limit the business associate’s uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity’s minimum necessary policies and procedures. Given that a business associate contract must limit a business associate’s requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.

# Is a physician or other provider considered to be a business associate of a health plan or other payer?

### Answer:

Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. Each covered entity is acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. However, a business associate relationship could arise if the provider is performing another function on behalf of, or providing services to, the health plan (e.g., case management services) that meet the definition of “business associate” at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml).

# Is a health insurance issuer or HMO who provides health insurance or health coverage to a group health plan a business associate of the group health plan?

### Answer:

A health insurance issuer or HMO does not become a business associate simply by providing health insurance or health coverage to a group health plan. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an organized health care arrangement (OHCA), with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA. However, where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the joint activity of providing insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities, or services.

# Is a reinsurer a business associate of a health plan?

### Answer:

Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. Each entity is acting on its own behalf when the health plan purchases the reinsurance benefits, and when the health plan submits a claim to a reinsurer and the reinsurer pays the claim.

However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.

# Is a software vendor a business associate of a covered entity?

### Answer:

The mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information of the [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html). If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity.

For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function, is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a business associate agreement before allowing the software company access to protected health information. However, when an employee of a contractor, like a software or information technology vendor, has his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity’s workforce, rather than as a business associate. See the definition of “workforce” at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml).

# When a covered entity, such as a doctor, uses a certified Telecommunications Relay Service to contact patients with hearing or speech impairments, is the Relay Service a business associate of the doctor?

### Answer:

Under the Privacy Rule, a covered entity such as a doctor can contact a patient using a Telecommunications Relay Service (TRS), without the need for a business associate contract with the TRS. The sharing of protected health information between a covered health care provider and a patient through the TRS is permitted by the Privacy Rule under 45 C.F.R. 164.510(b), and a business associate contract is not required in these circumstances.

By way of background, the TRS enables telephone communication for people with hearing or speech impairments by using a communications assistant (CA) who transliterates conversations. The TRS CA relays information, which may include protected health information, between a text telephone (also known as “TTY”) user and another person communicating via voice. The CA must communicate what is said by the parties without alteration. The Federal Communications Commission (FCC), pursuant to the Americans with Disabilities Act (ADA), certifies all State TRS programs, which in turn contract with one or more TRS providers. All TRS providers must comply with standards for operators established by the FCC pursuant to Title IV of the ADA, including protecting the privacy of all relayed communications. The TRS is a public service that is available without cost to all persons and businesses, none of whom need to employ, contract with or otherwise establish business relationships with the TRS. Thus, when performing these services, the TRS is not acting for or on behalf of the covered entity and is not the covered entity’s business associate.

As permitted by [45 C.F.R. 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b), protected health information can be shared during a telephone communication using the TRS because the individual will have an opportunity to agree or object to disclosures of protected health information to the CA. The following typical scenarios describe how this opportunity can be provided in the course of, or prior to, using the TRS:

* Where the individual initiates the call through the TRS, it is reasonable for a covered health care provider to infer from these circumstances that the individual has identified the CA as involved in the individual’s care, and that the individual does not object to the disclosure. See [45 C.F.R. 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b)(2)(iii).
* Where the need for use of the TRS becomes apparent prior to a call being placed, such as when, during an office visit, the individual gives the health care provider his or her TTY number, the opportunity to agree or object to the TRS can be provided at that time. See 45 C.F.R. 164.510(b)(2).
* Even where the covered health care provider initiates a call using the TRS without the individual’s prior agreement, the individual will have an opportunity to agree or object at the outset of the call. Typically, the CA will begin the call by identifying the service to the party called, and if that party is unfamiliar with the TRS, the CA will briefly explain how the service operates. This initial contact by the CA provides the individual with the opportunity to agree to the disclosure by proceeding with the call using the TRS, or to object by terminating the call. See 45 C.F.R. 164.510(b)(2)(i)-(ii).

# In providing legal services to a covered entity, must a lawyer who is a business associate require that those persons to whom it discloses protected health information agree to abide by the privacy restrictions and conditions that apply to the lawyer?

### Answer

It depends on who the recipient is. The business associate agreement between the [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) and the lawyer-business associate must provide that the lawyer will ensure that any agents, including subcontractors, to whom it provides protected health information agree to the same restrictions and conditions that apply to the business associate with respect to the information. See [45 CFR 164.504(e)(2)(ii)(D)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml).

Thus, if a lawyer-business associate enlists the services of a person or entity in furtherance of the lawyer’s legal services to a covered entity, and the lawyer must provide protected health information to the person or entity for such purpose, the lawyer’s business associate contract with the covered entity requires that the lawyer ensure that these persons agree to the same restrictions and conditions with respect to the protected health information they receive that apply to the lawyer as a business associate.

For example, pursuant to its business associate contract, a lawyer must ensure that other legal counsel, jury experts, document or file managers, investigators, litigation support personnel, or others hired by the lawyer to assist the lawyer in providing legal services to the covered entity, will also safeguard the privacy of the protected health information the lawyer receives to perform its duties. Conversely, a lawyer-business associate need not ensure that opposing counsel, fact witnesses, or other persons who do not perform functions or services that assist the lawyer in performing its services to the client, agree to the business associate restrictions and conditions, even though the lawyer may have to disclose protected health information to these third parties.

# Does the HIPAA Privacy Rule require a business associate to provide individuals with access to their protected health information or an accounting of disclosures, or an opportunity to amend protected health information?

### Answer

The Privacy Rule regulates covered entities, not business associates. The Rule requires covered entities to include specific provisions in agreements with business associates to safeguard protected health information, and addresses how covered entities may share this information with business associates. Covered entities are responsible for fulfilling Privacy Rule requirements with respect to individual rights, including the rights of access, amendment, and accounting, as provided for by [45 CFR 164.524](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-524.xml), [164.526](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-526.xml), and [164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml). With limited exceptions, a covered entity is required to provide an individual access to his or her protected health information in a designated record set. This includes information in a designated record set of a business associate, unless the information held by the business associate merely duplicates the information maintained by the covered entity. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must make such protected health information available if and when needed by the covered entity to provide an individual with access to the information. However, the Privacy Rule does not prevent the parties from agreeing through the business associate contract that the business associate will provide access to individuals, as may be appropriate where the business associate is the only holder of the designated record set, or part thereof.

Under [45 CFR 164.526](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-526.xml), a covered entity must amend protected health information about an individual in a designated record set, including any designated record sets (or copies thereof) held by a business associate. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must amend protected health information in such records (or copies) when requested by the covered entity. The covered entity itself is responsible for addressing requests from individuals for amendment and coordinating such requests with its business associate. However, the Privacy Rule also does not prevent the parties from agreeing through the contract that the business associate will receive and address requests for amendment on behalf of the covered entity.

Under [45 CFR 164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml), the Privacy Rule requires a covered entity to provide an accounting of certain disclosures, including certain disclosures by its business associate, to the individual upon request. The business associate contract must provide that the business associate will make such information available to the covered entity in order for the covered entity to fulfill its obligation to the individual. As with access and amendment, the parties can agree through the business associate contract that the business associate will provide the accounting to individuals, as may be appropriate given the protected health information held by, and the functions of, the business associate.

# May a business associate of a HIPAA covered entity block or terminate access by the covered entity to the protected health information (PHI) maintained by the business associate for or on behalf of the covered entity?

### Answer:

No.

First, a business associate may not use PHI in a manner or to accomplish a purpose or result that would violate the HIPAA Privacy Rule. See 45 CFR § 164.502(a)(3). Generally, if a business associate blocks access to the PHI it maintains on behalf of a covered entity, including terminating access privileges of the covered entity, the business associate has engaged in an act that is an impermissible use under the Privacy Rule. For example, a business associate blocking access by a covered entity to PHI (such as where an Electronic Health Record (EHR) developer activates a “kill switch” embedded in its software that renders the data inaccessible to its provider client) to resolve a payment dispute with the covered entity is an impermissible use of PHI. Similarly, in the event of termination of the agreement by either party, a business associate must return PHI as provided for by the business associate agreement. If a business associate fails to do so, it has impermissibly used PHI.

Second, a business associate is required by the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of all electronic PHI (ePHI) that it creates, receives, maintains, or transmits on behalf of a covered entity. See 45 CFR § 164.306(a)(1). Maintaining the availability of the ePHI means ensuring the PHI is accessible and usable upon demand by the covered entity, whether the PHI is maintained in an EHR, cloud, data backup system, database, or other system. 45 CFR § 164.304. This also includes, in cases where the business associate agreement specifies that PHI is to be returned at termination of the agreement, returning the PHI to the covered entity in a format that is reasonable in light of the agreement to preserve its accessibility and usability. A business associate that terminates access privileges of a covered entity, or otherwise denies a covered entity’s access to the ePHI it holds on behalf of the covered entity, is violating the Security Rule.

Third, a business associate is required by the HIPAA Privacy Rule and its business associate agreement to make PHI available to a covered entity as necessary to satisfy the covered entity’s obligations to provide access to individuals under 45 CFR § 164.524. See 45 CFR §§ 164.502(a)(4)(ii), 164.504(e)(2)(ii)(E). Therefore, a business associate may not deny a covered entity access to the PHI the business associate maintains on behalf of the covered entity if the covered entity needs the PHI to satisfy its obligations under 45 CFR § 164.524.

OCR recognizes, however, that there may be certain arrangements that authorize the business associate to destroy or dispose of PHI, or perform data aggregation or otherwise combine data from multiple sources, and where, because of the nature of the services to be performed by the business associate with the PHI as specified in the contractual arrangements between the parties, the covered entity and business associate agree that the business associate will not provide the covered entity access to the PHI. For example, a covered entity may engage a business associate to perform data aggregation of information from multiple sources that renders the disaggregated original source data unreturnable to the covered entity. OCR does not consider these contractual arrangements to constitute the types of impermissible data blocking or access termination described above.

Finally, OCR notes that a covered entity is responsible for ensuring the availability of its own PHI. To the extent that a covered entity has agreed to terms in a business associate agreement that prevent the covered entity from ensuring the availability of its own PHI, whether in paper or electronic form, the covered entity is not in compliance with 45 CFR §§ 164.308(b)(3), 164.502(e)(2), and 164.504(e)(1).

Under the HIPAA Privacy Rule, may a covered entity contract with a business associate to create a limited data set the same way it can use a business associate to create de-identified data?

Answer:

Yes. See 45 CFR 164.514(e)(3)(ii). For example, if a researcher needs county data, but the covered entity’s data contains only the postal address of the individual, a business associate may be used to convert the covered entity’s geographical information into that needed by the researcher. In addition, the covered entity may hire the intended recipient of the limited data set as the business associate for this purpose in accordance with the business associate requirements. That is, the covered entity may provide protected health information, including direct identifiers, to a business associate who is also the intended data recipient, to create a limited data set of the information responsive to the recipient’s request. However, the data recipient, as a business associate, must agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

I want to hire the intended recipient of a limited data set to also create the limited data set as my business associate. Can I combine the data and use agreement and business associate contract?

Answer:

Yes. A data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule. In the above situation, because the [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) is providing the recipient with protected health information that includes direct identifiers, a business associate agreement would be required in addition to the data use agreement to protect the information.

For example, the agreement must require that the recipient agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

# May a covered entity hire a business associate to create a limited data set, and may the public health authority be a business associate for that purpose, even if the public health authority is also the intended recipient of the limited data set?

### Answer:

A covered entity may enter into a business associate agreement with the public health authority for the sole purpose of creating a limited data set, even if the same public health authority is also the intended recipient of the information ([45 CFR 164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(e)(3)(ii)). For example, the covered entity may contract with the public health authority as a business associate for the exclusive purpose of reviewing medical charts and extracting the facially unidentifiable information needed for the particular public health surveillance activity. In these cases, the public health authority, as the covered entity’s business associate for purposes of creating a limited data set, must agree to return, destroy or not remove from the covered entity’s premises the protected health information that includes the direct identifiers, once the public health authority has completed the conversion of the information into a limited data set for its own public health use. Because the public health authority is not only the covered entity’s business associate for creating the limited data set, but also the intended recipient of the limited data set, the public health authority must enter into both a data use agreement and a business associate agreement. The data use agreement can be combined with the business associate agreement into a single agreement so long as the agreement meets the requirements of both provisions. See [45 CFR 164.504](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml)(e)(2) and [164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(e)(4).

While there are two disclosures in this case – the disclosure to the public health authority in its role as the covered entity’s business associate in creating the limited data set, and the disclosure to the public health authority as the recipient of the limited data set – neither disclosure requires an accounting. A disclosure to a business associate for the purpose of creating a limited data set is a health care operation, as defined by the Rule at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml). Disclosures for health care operations and disclosures made as a limited data set are both excepted from the accounting requirement at [45 CFR 164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml)(a)(1)(i) and (viii), respectively.

# Was the Privacy Rule compliance date delayed by the Administrative Simplification Compliance Act (ASCA) that was enacted in December 2001?

### Answer:

No, the compliance date for the Privacy Rule was April 14, 2003, or, for small health plans, April 14, 2004. ASCA does not apply to the HIPAA Privacy Rule. Rather, ASCA delays compliance with the Transaction and Code Set standards adopted by the HIPAA Transactions Rule for [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) that file a compliance plan.

More information about ASCA can be found on the web site for the [Centers for Medicare and Medicaid Services](http://www.cms.hhs.gov/HIPAAGenInfo/02_TheHIPAALawandRelated%20Information.asp).

# Who must comply with HIPAA privacy standards?

### Answer:

As required by Congress in HIPAA, the Privacy Rule covers:

* Health plans
* Health care clearinghouses
* Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

These entities (collectively called “[covered entities](https://www.hhs.gov/ocr/privacy/hipaa/faq/right_to_an_accounting_of_disclosures/204.html)”) are bound by the privacy standards even if they contract with others (called “business associates”) to perform some of their essential functions. The law does not give the Department of Health and Human Services (HHS) the authority to regulate other types of private businesses or public agencies through this regulation. For example, HHS does not have the authority to regulate employers, life insurance companies, or public agencies that deliver social security or welfare benefits. See our [business associate section](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html) and the [frequently asked questions about business associates](https://www.hhs.gov/hipaa/for-professionals/faq/business-associates) for a more detailed discussion of the covered entities’ responsibilities when they engage others to perform essential functions or services for them.

# Are state, county or local health departments required to comply with the HIPAA Privacy Rule?

### Answer:

Yes, if a State, county, or local health department performs functions that make it a covered entity, or otherwise meets the definition of a covered entity they must comply with the HIPAA Privacy Rule. For example, a state Medicaid program is a covered entity (i.e., a health plan) as defined in the Privacy Rule. Some health departments operate health care clinics and thus are health care providers. If these health care providers transmit health information electronically in connection with a transaction covered in the HIPAA Transactions Rule, they are covered entities.

For more information, see the definitions of covered entity, health care provider, health plan and health care clearinghouse in [45 CFR 160.103](http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr160_07.html). See also the [Disclosures for Emergency Preparedness - A Decision Tool](https://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/decisiontoolintro.html).

This tool addresses the question of whether a person, business or agency is a covered health care provider, health care clearinghouse or health plan. If the health department performs some covered functions (i.e., those activities that make it a provider that conducts certain transactions electronically, a health plan or a health care clearinghouse) and other non-covered functions, it may designate those components (or parts thereof) that perform covered functions as the health care component(s) of the organization and thereby become a type of covered entity known as a “hybrid entity.” Most of the requirements of the Privacy Rule apply only to the hybrid entity’s health care component(s). If a health department elects to be a hybrid entity, there are restrictions on how its health care component(s) may disclose protected health information to other components of the health department. See 45 CFR 164.103 and 164.105 for more information about hybrid entities.

# Are the following types of insurance covered under HIPAA: long/short term disability; workers' compensation; automobile liability that includes coverage for medical payments?

### Answer:

No, the listed types of policies are not health plans. The HIPAA Administrative Simplification regulations specifically exclude from the definition of a “health plan” any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits, which are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1). See 45 CFR 160.103. As described in the statute, excepted benefits are one or more (or any combination thereof) of the following policies, plans or programs:

* Coverage only for accident, or disability income insurance, or any combination thereof.
* Coverage issued as a supplement to liability insurance.
* Liability insurance, including general liability insurance and automobile liability insurance.
* Workers’ compensation or similar insurance.
* Automobile medical payment insurance.
* Credit-only insurance.
* Coverage for on-site medical clinics
* Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

# Is an entity that is acting as a third party administrator to a group health plan a covered entity?

### Answer:

No, providing services to or acting on behalf of a health plan does not transform a third party administrator (TPA) into a covered entity. Generally, a TPA of a group health plan would be acting as a business associate of the group health plan. Of course, the TPA may meet the definition of a covered entity based on its other activities (such as by providing group health insurance). See [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml)(GPO).

# The Social Security Administration (SSA) collects medical records when making disability determinations for both title II (Disability Insurance) and title XVI (Supplemental Security Income, SSI) of the Social Security Act. Is SSA a covered entity (e.g., a health plan)?

### Answer:

The Social Security Administration (SSA) is not a covered entity. The collection of individually identifiable health information is not a factor in determining whether an entity is a covered entity. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) are defined in HIPAA; they are

1. health plans,
2. health care clearinghouses, and
3. health care providers that transmit any health information in electronic form in connection with a transaction covered in the HIPAA Transactions Rule.

SSA meets none of these criteria as defined at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml) (GPO).

# Is a flexible spending account or a cafeteria plan a covered entity for purposes of the Privacy Rule and the other HIPAA, Title II, Administrative Simplification standards?

### Answer:

A "group health plan" is a covered entity under the Privacy Rule and the other HIPAA, Title II, Administrative Simplification standards. A "group health plan" is defined as an "employee welfare benefit plan," as that term is defined by the Employee Retirement Income Security Act (ERISA), to the extent that the plan provides medical care. See [42 USC § 1320d(5)(A)](http://www.justice.gov/sites/default/files/olc/opinions/attachments/2014/11/17/hipaa_final.htm) (DOJ) and [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml)(GPO). Thus, to the extent that a flexible spending account or a cafeteria plan meets the definition of an employee welfare benefit plan under ERISA and pays for medical care, it is a group health plan, unless it has fewer than 50 participants and is self-administered. Employee welfare benefit plans with fewer than 50 participants and that are self-administered are not group health plans. Flexible spending accounts and cafeteria plans are not excluded from the definition of "health plan" as excepted benefits. See [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml) (GPO), paragraph (2)(i) of the definition of "health plan."

# Must all small health plans comply with the Privacy Rule?

### Answer:

No. Certain plans are specifically excluded from having to comply with the HIPAA Administrative Simplification requirements, including the Privacy Rule. See [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml) (GPO). An employee welfare benefit plan that has less than 50 participants and is administered by the employer that establishes and maintains the plan is not a HIPAA covered entity. These plans, therefore, are not subject to the Privacy Rule. For additional information regarding compliance with the Privacy Rule, see the [Office for Civil Rights Web site](https://www.hhs.gov/ocr/privacy/).

# I’m an employer that offers a fully insured group health plan for my employees. Is the fully insured group health plan subject to all of the Privacy Rule provisions?

### Answer:

The Privacy Rule recognizes that certain fully insured group health plans may not need to satisfy all of the requirements of the Privacy Rule since these responsibilities will be carried out by the health insurance issuer or HMO with which the group health plan has contracted for coverage of its members. In particular, a fully insured group health plan that does not create or receive protected health information other than summary health information (see definition at [45 CFR 164.504(a)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml) (GPO)) and enrollment or disenrollment information is not required to have or provide a notice of privacy practices. See [45 CFR 164.520(a)(2)](https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR) (GPO).

Moreover, these group health plans are exempt from most of the administrative responsibilities under the Privacy Rule. See [45 CFR 164.530(k)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-530.xml). These health plans are still required, however, to refrain from intimidating or retaliatory acts ([45 CFR 164.530(g)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-530.xml) (GPO)), and from requiring an individual to waive their privacy rights ([45 CFR 164.530(h)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-530.xml) (GPO)). The documentation requirements at 45 CFR 164.530(j) apply to these group health plans only to the extent of amendments, if any, made to the plan documents for the sharing of information with the plan sponsor under [45 CFR 164.504(f)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml) (GPO). Additional information about the Privacy Rule, including guidance and technical assistance materials is available through the Department of Health and Human Services [Office for Civil Rights Web site](https://www.hhs.gov/ocr/privacy/).

#

# As an employer, I sponsor a group health plan for my employees. Am I a covered entity under HIPAA?

### Answer:

Covered entities under HIPAA are health care clearinghouses, certain health care providers, and health plans. A "group health plan" is one type of health plan and is a covered entity (except for self-administered plans with fewer than 50 participants). The group health plan is considered to be a separate legal entity from the employer or other parties that sponsor the group health plan. Neither employers nor other group health plan sponsors are defined as covered entities under HIPAA.

Thus, the Privacy Rule does not directly regulate employers or other plan sponsors that are not HIPAA covered entities. However, the Privacy Rule does control the conditions under which the group health plan can share protected health information with the employer or plan sponsor when the information is necessary for the plan sponsor to perform certain administrative functions on behalf of the group health plan. See [45 CFR 164.504(f)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml). Among these conditions is receipt of a certification from the employer or plan sponsor that the health information will be protected as prescribed by the rule and will not be used for employment-related actions.

The covered group health plan must comply with Privacy Rule requirements, though these requirements will be limited when the group health plan is fully insured. See the Answer to the FAQ "Is a fully insured health plan subject to all Privacy Rule requirements?" That question, hundreds of FAQs, and a wide range of other guidance and materials to assist covered entities in complying with HIPAA and the Privacy Rule, are available at the Department of Health and Human Services [Office for Civil Rights Web site](https://www.hhs.gov/ocr/privacy/).

**Are tissue repositories covered entities?**

### Answer:

Not unless the organization maintaining the tissue repository conducts some other activity that makes it a covered entity. For example, tissue repositories that conduct testing of specimens for the benefit of transplant recipients based on another health care provider's orders would be covered providers under HIPAA if they conduct electronic transactions for which the HHS has adopted standards.

# How can family members of a deceased individual obtain the deceased individual's protected health information that is relevant to their own health care?

### Answer:

The HIPAA Privacy Rule recognizes that a deceased individual’s protected health information may be relevant to a family member’s health care. The Rule provides two ways for a surviving family member to obtain the protected health information of a deceased relative.

First, disclosures of protected health information for treatment purposes—even the treatment of another individual—do not require an authorization; thus, a covered entity may disclose a decedent’s protected health information, without authorization, to the health care provider who is treating the surviving relative.

Second, a [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp%20) must treat a deceased individual’s legally authorized executor or administrator, or a person who is otherwise legally authorized to act on the behalf of the deceased individual or his estate, as a personal representative with respect to protected health information relevant to such representation.

Therefore, if it is within the scope of such personal representative’s authority under other law, the Rule permits the personal representative to obtain the information or provide the appropriate authorization for its disclosure.

# Do the HIPAA Privacy Rule protections apply to the health information of deceased individuals?

### Answer:

Yes, for a period of 50 years following the date of death of the individual.  During this period, the Privacy Rule protects the identifiable health information of the deceased individual to the same extent the Rule protects the health information of a living individual.  However, in cases where a covered entity maintains a medical records archive or otherwise maintains health or medical records that contain identifiable health information on individuals who have been deceased for more than 50 years, such information is not considered protected health information and may be used or disclosed without regard to the Privacy Rule.

# Since the HIPAA Privacy Rule protects a decedent’s health information for 50 years following the individual’s death, am I required to keep the decedent’s information for that period of time?

### Answer:

No.  The Privacy Rule does not include medical record retention requirements and covered entities may destroy such records at the time permitted by State or other applicable law.

# Since the HIPAA Privacy Rule protects a decedent’s health information only for 50 years following the individual’s death, does my family health history recorded in my medical record lose protection when it involves family members who have been deceased for more than 50 years?

### Answer:

No. When a covered health care provider, in the course of treating an individual or otherwise, collects an individual’s family health history, this information becomes part of the individual’s medical or other record and is treated as protected health information about the individual and not about the family member(s). Thus, even where an individual’s family health history includes information about family members who have been deceased for more than 50 years, the information is protected under the Privacy Rule as the health information of the individual.

# Does the HIPAA Privacy Rule permit a covered entity to disclose protected health information about a decedent to family members or other persons involved in the care of the decedent?

### Answer:

Yes. The Privacy Rule permits a covered entity to disclose protected health information about a decedent to a family member, or other person who was involved in the individual’s health care or payment for care prior to the individual’s death, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity. This may include, depending on the circumstances, disclosures to spouses, parents, children, domestic partners, other relatives, or friends of the decedent, provided the information disclosed is limited to that which is relevant to the person’s involvement in the decedent’s care or payment for care. See 45 CFR 164.510(b)(5). For example, a covered health care provider could describe the circumstances that led to an individual’s death with the decedent’s sister who is asking about her sibling’s death.  In addition, a covered health care provider or pharmacy could disclose billing information or records to a family member of a decedent who is assisting with closing a decedent’s estate. However, in both cases, a provider generally should not share information about past, unrelated medical problems.

# If an individual instructs a covered health care provider that he does not want the provider to discuss his medical conditions or treatment with his family members, can the covered entity share such information with family members after the individual has died?

### Answer:

Generally, no.  The Privacy Rule permits a covered entity to disclose protected health information about a decedent to a family member, or other person who was involved in the decedent’s health care or payment for care prior to the decedent’s death, only if doing so is not inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity.  However, a family member that is a personal representative of the decedent (e.g., an executor or administrator of the decedent’s estate) is to be treated as the individual for purposes of the Privacy Rule with respect to protected health information relevant to the representation.  In these cases, a covered health care provider may disclose relevant protected health information about the decedent to the family member, and the family member retains the right to receive a copy of the relevant information in the decedent’s medical record, without regard to the decedent’s prior objection.

# How can a covered entity determine whether a person is a family member, or person involved in an individual’s care prior to death, for purposes of sharing protected health information about the decedent after death?

### Answer:

In some cases, it will be readily apparent to the covered entity that a person is a family member, or was involved in the individual’s care prior to death, because the person would have made themselves known to the covered entity prior to the individual’s death by either visiting with or inquiring about the individual, or the individual would have identified such person as being a family member, or other person involved in his or her care or payment for care, to a member of the covered entity’s workforce.  In other cases, the covered entity need just have reasonable assurance that the person is a family member of the decedent or other person who was involved in the individual’s care or payment for care prior to death.  For example, the person may indicate to the covered entity how he or she is related to the decedent or offer sufficient details about the decedent’s circumstances prior to death to indicate involvement in the decedent’s care prior to death.  The Privacy Rule does not require formal verification of the identity and authority of the person but rather permits the covered entity to rely on the exercise of professional judgment in making the disclosure.

# Does the HIPAA Privacy Rule require that a health care provider document a patient’s expressed preference not to have the provider discuss the details of her health care with her family?

### Answer:

No.  The Privacy Rule does not require that a health care provider document a patient’s expressed preference not to have the provider discuss the details of the patient’s medical conditions or health care with family members of the patient.  However, while not required, we expect many providers do so (e.g., by making a note in the patient’s medical file) as a means of ensuring the provider does not later violate the Rule by making such a disclosure. Such notes also would ensure that all current and future members of the workforce who are in a position to make such disclosures are aware of the individual’s objection.

# Does the HIPAA Privacy Rule require my doctor to send my medical records to the government?

### Answer:

No. The Rule does not require a physician or any other [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to send medical information to the government for a government data base or similar operation. This Rule does not require or allow any new government access to medical information, with one exception: the Rule does give the Department of Health and Human Services Office for Civil Rights (OCR) the authority to investigate complaints that Privacy Rule protections or rights have been violated, and otherwise to ensure that covered entities comply with the Rule.

For enforcement purposes, OCR may need to look at how a covered entity handled medical records and other personal health information, as is typical in many enforcement settings. This investigative authority is needed so that the Rule can be enforced, and to ensure the independent review of consumers’ concerns over privacy violations.

Even so, the Privacy Rule limits disclosures to OCR to information that is “pertinent to ascertaining compliance.” OCR will maintain stringent controls to safeguard any individually identifiable health information that it receives. If covered entities could avoid or ignore enforcement requests, consumers would not have a way to ensure an independent review of their concerns about privacy violations under the Rule.

# Why would HIPAA Privacy Rule require covered entities to turn over anybody's personal health information as part of a government enforcement process?

### Answer:

An important ingredient in ensuring compliance with the Privacy Rule is the Department of Health and Human Services’ (HHS) responsibility to investigate complaints that the Rule has been violated and to follow up on other information regarding noncompliance. At times, this responsibility entails seeing personal health information, such as when an individual indicates to the Department that they believe a covered entity has not properly handled their medical records.

What information would be needed depends on the circumstances and the alleged violations. The Privacy Rule limits HHS Office for Civil Rights’ (OCR) access to information that is “pertinent to ascertaining compliance.” In some cases, no personal health information may be needed. For instance, OCR would need to review only a business contract to determine whether a health plan included appropriate language to protect privacy when it hired an outside company to help process claims.

Examples of investigations that may require OCR to have access to protected health information include:

* Allegations that a covered entity refused to note a request for correction in a patient’s medical record, or did not provide complete access to a patient’s medical records to that patient.
* Allegations that a covered entity used health information for marketing purposes without first obtaining the individuals’ authorization when required by the Rule. OCR may need to review information in the marketing department that contains personal health information, to determine whether a violation has occurred.

# Will this HIPAA Privacy Rule make it easier for police and law enforcement agencies to get my medical information?

### ****Answer:****

No. The Rule does not expand current law enforcement access to individually identifiable health information. In fact, it limits access to a greater degree than currently exists, since the Rule establishes new procedures and safeguards that restrict the circumstances under which a covered entity may give such information to law enforcement officers.

For example, the Rule limits the type of information that [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Similarly, under most circumstances, the Privacy Rule requires covered entities to obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement.

In most States, such permission is not required today. Where State law imposes additional restrictions on disclosure of health information to law enforcement, those State laws continue to apply. This Rule sets a national floor of legal protections; it is not a set of “best practices.” Even in those circumstances when disclosure to law enforcement is permitted by the Rule, the Privacy Rule does not require covered entities to disclose any information. Some other Federal or State law may require a disclosure, and the Privacy Rule does not interfere with the operation of these other laws. However, unless the disclosure is required by some other law, covered entities should use their professional judgment to decide whether to disclose information, reflecting their own policies and ethical principles. In other words, doctors, hospitals, and health plans could continue to follow their own policies to protect privacy in such instances.

# Does the HIPAA Privacy Rule permit covered entities to disclose protected health information, without individuals' authorization, to public officials responding to a bioterrorism threat or other public health emergency?

### Answer:

Yes. The Rule recognizes that various agencies and public officials will need protected health information to deal effectively with a bioterrorism threat or emergency. To facilitate the communications that are essential to a quick and effective response to such events, the Privacy Rule permits [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to disclose needed information to public officials in a variety of ways.

Covered entities may disclose protected health information, without the individual's authorization, to a public health authority acting as authorized by law in response to a bioterrorism threat or public health emergency (see [45 CFR 164.512(b))](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html), public health activities). The Privacy Rule also permits a covered entity to disclose protected health information to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism (see 45 CFR 164.512(j)), to avert a serious threat to health or safety). In addition, disclosure of protected health information, without the individual's authorization, is permitted where the circumstances of the emergency implicates law enforcement activities (see [45 CFR 164.512(f)](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/restrictions-on-government-access-to-health-information/index.html)); national security and intelligence activities (see 45 CFR 164.512(k)(2)); or judicial and administrative proceedings (see 45 CFR 164.512(e)).

# When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?

### Answer:

The Privacy Rule is balanced to protect an individual’s privacy while allowing important law enforcement functions to continue. The Rule permits [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to disclose protected health information (PHI) to law enforcement officials, without the individual’s written authorization, under specific circumstances summarized below. For a complete understanding of the conditions and requirements for these disclosures, please review the exact regulatory text at the citations provided. Disclosures for law enforcement purposes are permitted as follows:

* **To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.** The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual’s private information ([45 CFR 164.512(f)(1)(ii)(A)-(B)](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)).
* **To respond to an administrative request***,* such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used (45 CFR 164.512(f)(1)(ii)(C)).
* **To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures** of PHI to name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. Other information related to the individual’s DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request (45 CFR 164.512(f)(2)).

**This same limited information may be reported to law enforcement:**

* + **About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity’s workforce** (45 CFR 164.502(j)(2));
	+ **To identify or apprehend an individual who has admitted participation in a violent crime**that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual’s request for therapy, counseling, or treatment related to the propensity to commit this type of violent act (45 CFR 164.512(j)(1)(ii)(A), (j)(2)-(3)).
* **To respond to a request for PHI about a victim of a crime, and the victim agrees***.* If, because of an emergency or the person’s incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested (45 CFR 164.512(f)(3)).

Where child abuse victims or adult victims of abuse, neglect or domestic violence are concerned, other provisions of the Rule apply:

* + **Child abuse or neglect may be reported** to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required (45 CFR 164.512(b)(1)(ii)).
	+ **Adult abuse, neglect, or domestic violence may be reported** to a law enforcement official authorized by law to receive such reports (45 CFR 164.512(c)):
		- If the individual agrees;
		- If the report is required by law; or
		- If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations (see 45 CFR 164.512(c)(1)(iii)(B)).
		- Notice to the individual of the report may be required (see 45 CFR 164.512(c)(2)).
* **To report PHI to law enforcement when required by law** to do so (45 CFR 164.512(f)(1)(i)). For example, state laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.
* **To alert law enforcement to the death of the individual***,* when there is a suspicion that death resulted from criminal conduct (45 CFR 164.512(f)(4)).
	+ Information about a decedent may also be shared with **medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties***(45 CFR 164.512(g)(1)).*
* **To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity’s premises** (45 CFR 164.512(f)(5)).
* **When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity,** specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime (45 CFR 164.512(f)(6)). This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence; see above Adult abuse, neglect, or domestic violence for when reports to law enforcement are allowed under 45 CFR 164.512(c).
* When consistent with applicable law and ethical standards:
	+ To a law enforcement official reasonably able to **prevent or lessen a serious and imminent threat to the health or safety of an individual or the public** (45 CFR 164.512(j)(1)(i)); or
	+ **To identify or apprehend an individual who appears to have escaped from lawful custody**(45 CFR 164.512(j)(1)(ii)(B))*.*
* **For certain other specialized governmental law enforcement purposes***,* such as:
	+ **To federal officials authorized to conduct** intelligence, counter-intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3));
	+ **To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody** of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the health and safety of the individual, other inmates, officers or employees of or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility (45 CFR 164.512(k)(5)).

Except when required by law, the disclosures to law enforcement summarized above are subject to a minimum necessary determination by the covered entity (45 CFR 164.502(b), 164.514(d)). When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose (45 CFR 164.514(d)(3)(iii)(A)). Moreover, if the law enforcement official making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information (45 CFR 164.514(h)).

# State public records laws, also known as open records or freedom of information laws, all provide for certain public access to government records. How does the HIPAA Privacy Rule relate to these state laws?

### Answer:

If a state agency is not a “covered entity”, as that term is defined at 45 CFR 160.103, it is not required to comply with the HIPAA Privacy Rule and, thus, any disclosure of information by the state agency pursuant to its state public records law would not be subject to the Privacy Rule.

If a state agency is a covered entity, however, the Privacy Rule applies to its disclosures of protected health information. The Privacy Rule permits a covered entity to use and disclose protected health information as required by other law, including state law. See 45 CFR 164.512(a). Thus, where a state public records law mandates that a covered entity disclose protected health information, the covered entity is permitted by the Privacy Rule to make the disclosure, provided the disclosure complies with and is limited to the relevant requirements of the public records law.

However, where a state public records law only permits, and does not mandate, the disclosure of protected health information, or where exceptions or other qualifications apply to exempt the protected health information from the state law’s disclosure requirement, such disclosures are not “required by law” and thus, would not fall within § 164.512(a) of the Privacy Rule. For example, if a state public records law includes an exemption that affords a state agency discretion not to disclose medical or other information where such disclosure would constitute a clearly unwarranted invasion of personal privacy, the disclosure of such records is not required by the public records law, and therefore is not permissible under § 164.512(a). In such cases, a covered entity only would be able to make the disclosure if permitted by another provision of the Privacy Rule.

As an example of how the Privacy Rule would apply in the case where an exemption exists in a freedom of information law, see the December 2000 Privacy Rule preamble discussion regarding the relationship of the Privacy Rule with the federal Freedom of Information Act (64 FR 82482).

# May a health plan disclose protected health information to a state child support enforcement (IV-D) agency in response to a National Medical Support Notice?

### Answer:

The Privacy Rule permits a health plan to respond to a request for information by a IV-D agency pursuant to a National Medical Support Notice (NMSN), as described below.

The Privacy Rule at 45 CFR 164.512(f) permits a covered entity to disclose protected health information to a “law enforcement official” for law enforcement purposes in compliance with court orders, grand jury subpoenas, or certain written administrative requests. 45 CFR 164.512(f)(1)(ii). As defined in 45 CFR 164.501, a “law enforcement official” means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law or to prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. An employee of a IV-D agency, including a contract employee, who is empowered by state or federal law to enforce a medical child support order, meets this definition of a law enforcement official.

The NMSN, a nationally uniform form which is sent by the IV-D agency to the employer and health plan for completion, constitutes a written administrative request by a law enforcement official. As such, the Privacy Rule allows a health plan to disclose protected health information in response to the NMSN, provided it includes or is accompanied by written assurances by the law enforcement official that (1) the information sought is material and relevant to a legitimate law enforcement inquiry; (2) the request is specific and limited in scope; and (3) de-identified information cannot reasonably be used. 45 CFR 164.512(f)(1)(ii)(C).

The Privacy Rule requires the covered entity to verify that these three conditions are met, as well as the identity and authority of the public official making the request, unless already known to the covered entity. The covered entity must also limit the disclosures to the minimum necessary for the purpose. To meet these requirements, the covered entity may reasonably rely on the following:

* the NMSN, or a separate written statement that, on its face, demonstrates that the three assurances required for these disclosures have been met. 45 CFR 164.514(h)(2)(i)(A).
* the NMSN is sufficient to verify the identity and legal authority of the public official requesting the protected health information. 45 CFR 164.514(h)(2)(ii) and (iii).
* the NMSN is sufficient as a request from a public official for the minimum information needed to meet the law enforcement purpose of the request. 45 CFR 164.514(d)(3)(iii)(A).

# Can health care information be shared in a severe disaster?

### Answer:

**Providers and health plans covered by the HIPAA Privacy Rule can share patient information in all of the following ways:**

**TREATMENT: Health care providers can share patient information as necessary to provide treatment.**

Treatment includes:

* sharing information with other providers (including hospitals and clinics),
* referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
* coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).

Providers can also share patient information to the extent necessary to seek payment for these health care services.

**NOTIFICATION: Health care providers can share patient information as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.**

The health care provider should get verbal permission from individuals, when possible; but if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgement, doing so is in the patient's best interest.

* Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify, or otherwise notify family members and others as to the location and general condition of their loved ones.
* In addition, when a health care provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.

**IMMINENT DANGER: Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public -- consistent with applicable law and the provider's standards of ethical conduct.**

**FACILITY DIRECTORY: Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.**

Of course, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information.

#  Is the HIPAA Privacy Rule suspended during a national or public health emergency?

### Answer:

No; however, the Secretary of HHS may waive certain provisions of the Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

#### What provisions may be waived

If the President declares an emergency or disaster *and* the Secretary declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the HIPAA Privacy Rule:

1. the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient’s care (45 CFR 164.510(b))
2. the requirement to honor a request to opt out of the facility directory (45 CFR 164.510(a))
3. the requirement to distribute a notice of privacy practices (45 CFR 164.520)
4. the patient's right to request privacy restrictions (45 CFR 164.522(a))
5. the patient's right to request confidential communications (45 CFR 164.522(b))

**When and to what entities does the waiver apply**

If the Secretary issues such a waiver, it only applies:

1. In the emergency area and for the emergency period identified in the public health emergency declaration.
2. To hospitals that have instituted a disaster protocol.  The waiver would apply to all patients at such hospitals.
3. For up to 72 hours from the time the hospital implements its disaster protocol.

When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours has not elapsed since implementation of its disaster protocol.

Regardless of the activation of an emergency waiver, the HIPAA Privacy Rule permits disclosures for treatment purposes and certain disclosures to disaster relief organizations. For instance, the Privacy Rule allows covered entities to share patient information with the American Red Cross so it can notify family members of the patient’s location.  See 45 CFR 164.510(b)(4).

# Are location information services of collection agencies, which are required under the Fair Debt Collection Practices Act, permitted under the HIPAA Privacy Rule?

### Answer:

“Payment” is broadly defined as activities by health plans or health care providers to obtain premiums or obtain or provide reimbursements for the provision of health care. The activities specified are by way of example and are not intended to be an exclusive listing. Billing, claims management, collection activities and related data processing are expressly included in the definition of “payment.” See the definition of “payment” at [45 CFR 164.501.](https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html)

Obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable, and, therefore, would constitute a payment activity. See [45 CFR 164.501.](https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html) The covered entity and its business associate would also have to comply with any limitations placed on location information services by the [Fair Debt Collection Practices Act](http://www.ftc.gov/os/statutes/fdcpajump.shtm) (Federal Trade Commission).

# Won't the HIPAA Privacy Rule's minimum necessary standard impede the ability of workers' compensation insurers, state administrative agencies, and employers to obtain the health information needed to pay injured or ill workers the benefits guaranteed them under State workers' compensation system?

### Answer:

No. The Privacy Rule is not intended to impede the flow of health information to those who need it to process or adjudicate claims, or coordinate care, for injured or ill workers under workers’ compensation systems. The minimum necessary standard generally requires [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to make reasonable efforts to limit uses and disclosures of, as well as requests for, protected health information to the minimum necessary to accomplish the intended purpose. For disclosures of protected health information made for [workers’ compensation purposes](https://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/workerscomp.html) under 45 CFR 164.512(l), the minimum necessary standard permits covered entities to disclose information to the full extent authorized by State or other law. In addition, where protected health information is requested by a State workers’ compensation or other public official for such purposes, covered entities are permitted reasonably to rely on the official’s representations that the information requested is the minimum necessary for the intended purpose. See 45 CFR 164.514(d)(3)(iii)(A).

For disclosures of protected health information for payment purposes, covered entities may disclose the type and amount of information necessary to receive payment for any health care provided to an injured or ill worker.

The minimum necessary standard does not apply to disclosures that are required by State or other law or made pursuant to the individual’s authorization.

# I am a health care provider and my state law says I have to provide a workers' compensation insurer, upon request, with an injured workers' records that related to treatment or hospitalization for which compensation is being sought. Am I permitted to disclose the information required by my state law?

### Answer:

Yes. The HIPAA Privacy Rule permits a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to disclose protected health information as necessary to comply with State law. No minimum necessary determination is required. See 45 CFR 164.512(a) and [164.502(b)](http://akatest3-ion-www.hhs.gov.edgekey-staging.net/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html).

# My state requires consent to use or disclose health information. Does the HIPAA Privacy Rule take away this protection?

### Answer:

No. The Privacy Rule does not prohibit a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) from obtaining an individual's consent to use or disclose his or her health information and, therefore, presents no barrier to the entity's ability to comply with State law requirements.

# Does the HIPAA Privacy Rule permit nursing homes and other health care institutions to disclose information concerning admissions of supplemental security income (SSI) recipients to the Social Security Administration (SSA)?

### Answer:

Yes. SSA requires nursing homes, extended care facilities, and intermediate care facilities to report to SSA, within 2 weeks, admissions information about anyone receiving SSI who is admitted to the institution. The purpose of these reporting requirements is to prevent SSI overpayments caused by a SSI recipient’s failure to timely report changes in eligibility.

These requirements are stated in the Social Security Act (42 U.S.C. 1383(e)(1)(C)), and communicated through SSA’s guidance and other implementation materials. The Privacy Rule permits [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)to disclose protected health information without the individual’s authorization as required to comply with this law. See 45 CFR 164.512(a).

# May a covered entity disclose protected health information to a Protection and Advocacy system where the disclosure is required by law?

### Answer:

Yes. The Privacy Rule permits a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to disclose protected health information (PHI) without the authorization of the individual to a state-designated Protection and Advocacy (P&A) system to the extent that such disclosure is required by law and the disclosure complies with the requirements of that law. 45 CFR 164.512(a). The Developmental Disabilities Assistance and Bill of Rights Act (DD Act) provides for each state to designate a public or private entity as the Protection and Advocacy system to protect and advocate for the rights of individuals with developmental disabilities, including investigating incidents of abuse or neglect. The P&A designated pursuant to the DD Act is also the Protection and Advocacy system for purposes of the Protection and Advocacy for Individuals with Mental Illness Act (PAIMI Act) and is empowered to protect and advocate for the rights of individuals with mental illness. These statutes and their implementing regulations require that access to records be provided to P&As under certain circumstances. See the DD Act at 42 USCA 15043(a)(2)(I) and (J) and the PAIMI Act at 42 USCA 10805(a)(4), and their implementing regulations at 45 CFR 1386.22 and 42 CFR 51.41, respectively. Thus, a covered entity may disclose PHI as required by the DD and PAIMI Acts to P&As requesting access to such records in carrying out their protection and advocacy functions under these Acts. Similarly, covered entities may disclose PHI to P&As where another federal, state or other law mandates such disclosures, consistent with the requirements in such law. Where disclosures are required by law, the Privacy Rule’s minimum necessary standard does not apply, since the law requiring the disclosure will establish the limits on what should be disclosed. Moreover, with respect to required by law disclosures, a covered entity cannot use the Privacy Rule as a reason not to comply with its other legal obligations.

Section 164.512(a)(2) provides that in making a “required by law” disclosure about adult abuse, neglect or domestic violence (section 164.512(c)), for judicial or administrative proceedings (section 164.512(e)), or for law enforcement purposes (section 164.512(f)), covered entities must also comply with any additional privacy requirements in these provisions that apply. However, none of the additional procedural protections in sections 164.512(c), (e) and (f) apply to the type of “required by law” disclosures to P&As under the provisions of the DD and PAIMI Acts discussed here.

# May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?

### Answer:

Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual’s privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual’s care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed. See [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b)(3).

In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, the Department considers a request to receive mailings from the covered entity in a closed envelope rather than by postcard to be a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests, absent extenuating circumstances. See [45 CFR 164.522](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-522.xml)(b)

# Can a patient have a friend or family member pick up a prescription for her?

### Answer:

Yes. A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient’s best interest in allowing a person, other that the patient, to pick up a prescription. See [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b). For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that he or she is involved in the individual’s care, and the HIPAA Privacy Rule allows the pharmacist to give the filled prescription to the relative or friend. The individual does not need to provide the pharmacist with the names of such persons in advance.

Does the HIPAA Privacy Rule permit hospitals and other health care facilities to inform visitors or callers about a patient’s location in the facility and general condition?

Answer:

Yes. Covered hospitals and other covered health care providers can use a facility directory to inform visitors or callers about a patient’s location in the facility and general condition. The Privacy Rule permits a covered hospital or other covered health care provider to maintain in a directory certain information about patients – patient name, location in the facility, health condition expressed in general terms that does not communicate specific medical information about the individual, and religious affiliation. The patient must be informed about the information to be included in the directory, and to whom the information may be released, and must have the opportunity to restrict the information or to whom it is disclosed, or opt out of being included in the directory. The patient may be informed, and make his or her preferences known, orally or in writing. The facility may provide the appropriate directory information – except for religious affiliation – to anyone who asks for the patient by name. Religious affiliation may be disclosed to members of the clergy, who are given additional access to directory information under the Rule. (See other FAQs at this site by searching on the term “clergy”.)

Even when, due to emergency treatment circumstances or incapacity, the patient has not been provided an opportunity to express his or her preference about how, or if, the information may be disclosed, directory information about the patient may still be made available if doing so is in the individual’s best interest as determined in the professional judgment of the provider, and would not be inconsistent with any known preference previously expressed by the individual. In these cases, as soon as practicable, the covered health care provider must inform the patient about the directory and provide the patient an opportunity to express his or her preference about how, or if, the information may be disclosed. See 45 CFR 164.510(a).

Does the HIPAA Privacy Rule permit a hospital to inform callers or visitors of a patient’s location and general condition in the emergency room, even if the patient’s information would not normally be included in the main hospital directory of admitted patients?

Answer:

Yes. The Privacy Rule permits [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to maintain more than one type of patient directory, and to maintain multiple versions of them, provided that the other requirements at [45 CFR 164.510(a)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/pdf/CFR-2003-title45-vol1-sec164-510.pdf) also are followed. For instance, emergency rooms that maintain directory information, even though separate from, or in a form different than, the hospital directory of admitted patients, may still disclose the information consistent with the requirements of the Privacy Rule. For further information about how this section of the Rule applies, see our other FAQs on this topic by searching on the term "directory."

# Can the fact that a patient has been "treated and released," or that a patient has died, be released as part of the facility directory?

### Answer:

Yes. The fact that a patient has been "treated and released," or that a patient has died, may be released as part of the directory information about the patient’s general condition and location in the facility, provided that the other requirements at 45 CFR 164.510(a) also are followed. For further information about how this section of the Rule applies, see our other FAQs on this topic by searching on the term "directory."

# Can the phone number of a patient’s room be released as part of the facility directory?

### Answer:

Yes. The phone number of the patient's room in the facility may be released as part of the directory information about the patient's location in the facility, provided that the other requirements at 45 CFR 164.510(a) also are followed. For further information about how this section of the Rule applies, see our other FAQs on this topic by searching on the term "directory."

# May a hospital or other covered entity notify a patient's family member or other person that the patient is at their facility?

### Answer:

Yes. The HIPAA Privacy Rule, at [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b), permits covered entities to notify, or assist in the notification of, family members, personal representatives, or other persons responsible for the care of the patient, of the patient’s location, general condition, or death. Where the patient is present, or is otherwise available prior to the disclosure, and has capacity to make health care decisions, the covered entity may notify family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also use or disclose this information to notify the family and these other persons if it can reasonably infer from the circumstances, based on professional judgment, that the patient does not object. Under these circumstances, for example:

* A doctor may call a patient’s wife to tell her that her husband was in a car accident and is being treated in the emergency room for minor injuries.
* A doctor may contact a pregnant patient’s husband to let him know that his wife arrived at the hospital in labor and is about to give birth.
* A nurse may contact the patient’s friend to let him know that his roommate broke his leg falling down the stairs, has had surgery, and is in recovery.

Even when the patient is not present or it is impracticable because of emergency or incapacity to ask the patient about notifying someone, a covered entity can still notify family and these other persons when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). For example, a doctor may, using such professional judgment, call the adult daughter of an incapacitated patient to inform her that her father suffered a stroke and is in the intensive care unit of a hospital.

# Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?

### Answer:

Yes. The HIPAA Privacy Rule at [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient’s care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment, that the patient does not object. Under these circumstances, for example:

* A doctor may give information about a patient’s mobility limitations to a friend driving the patient home from the hospital.
* A hospital may discuss a patient’s payment options with her adult daughter.
* A doctor may instruct a patient’s roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
* A physician may discuss a patient’s treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

Even when the patient is not present or it is impracticable because of emergency circumstances or the patient’s incapacity for the covered entity to ask the patient about discussing her care or payment with a family member or other person, a covered entity may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). Thus, for example:

* A surgeon may, if consistent with such professional judgment, inform a patient’s spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient’s progress and prognosis.
* A doctor may, if consistent with such professional judgment, discuss an incapacitated patient’s condition with a family member over the phone.

In addition, the Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient’s best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.

# May a doctor or hospital disclose protected health information to a person or entity that can assist in notifying a patient’s family member of the patient’s location and health condition?

### Answer:

Yes. The HIPAA Privacy Rule permits a covered doctor or hospital to disclose protected health information to a person or entity that will assist in notifying a patient’s family member of the patient’s location, general condition, or death. See 45 CFR 164.510(b)(1)(ii). The patient’s written authorization is not required to make disclosures to notify, identify, or locate the patient’s family members, his or her personal representatives, or other persons responsible for the patient’s care. Rather, where the patient is present, or is otherwise available prior to the disclosure, and has capacity to make health care decisions, the covered entity may disclose protected health information for notification purposes if the patient agrees or, when given the opportunity, does not object. The covered entity may also make the disclosure if it can reasonably infer from the circumstances, based on professional judgment, that the patient does not object. See 45 CFR 164.510(b)(2).

Even when the patient is not present or it is impracticable because of emergency or incapacity to ask the patient about notifying someone, a covered entity can still disclose a patient’s location, general condition, or death for notification purposes when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b)(3).

Under these circumstances, for example:

A doctor may share information about a patient’s condition with the American Red Cross for the Red Cross to provide emergency communications services for members of the U.S. military, such as notifying service members of family illness or death, including verifying such illnesses for emergency leave requests.

* A hospital may ask police to help locate and communicate with the family of an individual killed or injured in an accident.
* A hospital may contact a patient’s employer for information to assist in locating the patient’s spouse so that he/she may be notified about the hospitalization of the patient.

# Under the HIPAA Privacy Rule, may a health care provider disclose protected health information about an individual to another provider, when such information is requested for the treatment of a family member of the individual?

Yes. The HIPAA Privacy Rule permits a covered health care provider to use or disclose protected health information for treatment purposes. While in most cases, the treatment will be provided to the individual, the HIPAA Privacy Rule does allow the information to be used or disclosed for the treatment of others. Thus, the Rule does permit a doctor to disclose protected health information about a patient to another health care provider for the purpose of treating another patient (e.g., to assist the other health care provider with treating a family member of the doctor’s patient). For example, an individual’s doctor can provide information to the doctor of the individual’s family member about the individual’s adverse reactions to anesthetics prior to the family member undergoing surgery. These uses and disclosures are permitted without the individual’s written authorization or other agreement with the exception of disclosures of psychotherapy notes, which requires the written authorization of the individual.

However, the HIPAA Privacy Rule permits but does not require a covered health care provider to disclose the requested protected health information. Thus, the doctor with the protected health information may decline to share the information even if the Rule would allow it. The HIPAA Privacy Rule may also impose other limitations on these disclosures. Under 45 CFR § 164.522, individuals have the right to request additional restrictions on the use or disclosure of protected health information for treatment, payment, or health care operations purposes. If the health care provider has agreed to the requested restriction, then the doctor is bound by that agreement and (except in emergency treatment situations) would not be permitted to share the information. However, the health care provider maintaining the records does not have to agree to the requested restriction. For example, an individual who has obtained a genetic test may request that the health care provider not use or disclose the test results. If the health care provider agrees to the restriction, the information could not be shared with providers treating other family members who are seeking to identify their own genetic health risks.

# If I do not object, can my health care provider share or discuss my health information with my family, friends, or others involved in my care or payment for my care?

Yes.  As long as you do not object, your health care provider is allowed to share or discuss your health information with your family, friends, or others involved in your care or payment for your care.  Your provider may ask your permission, may tell you he or she plans to discuss the information and give you an opportunity to object, or may decide, using his or her professional judgment, that you do not object.  In any of these cases, your health care provider may discuss only the information that the person involved needs to know about your care or payment for your care.

Here are some examples:

* An emergency room doctor may discuss your treatment in front of your friend when you ask that your friend come into the treatment room.
* Your hospital may discuss your bill with your daughter who is with you at the hospital and has questions about the charges.
* Your doctor may talk to your sister who is driving you home from the hospital about your keeping your foot raised during the ride home.
* Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment.
* Your nurse may tell you that he or she is going to tell your brother how you are doing, and then your nurse may discuss your health status with your brother if you did not say that he or she should not.

BUT:

* Your nurse may not discuss your condition with your brother if you tell your nurse not to.

# If I am unconscious or not around, can my health care provider still share or discuss my health information with my family, friends, or others involved in my care or payment for my care?

Yes.  If you are not around or cannot give permission, your health care provider may share or discuss your health information with family, friends, or others involved in your care or payment for your care if he or she believes, in his or her professional judgment, that it is in your best interest.  When someone other than a friend or family member is asking about you, your health care provider must be reasonably sure that you asked the person to be involved in your care or payment for your care.  Your health care provider may share your information face to face, over the phone, or in writing, but may only share the information that the family member, friend, or other person needs to know about your care or payment for your care.

Here are some examples:

* A surgeon who did emergency surgery on you may tell your spouse about your condition, either in person or by phone, while you are unconscious.
* A pharmacist may give your prescription to a friend you send to pick it up.
* A doctor may discuss your drugs with your caregiver who calls your doctor with a question about the right dosage.

BUT:

* A nurse may not tell your friend about a past medical problem that is unrelated to your current condition.

Do I have to give my health care provider written permission to share or discuss my health information with my family members, friends, or others involved in my care or payment for my care?

HIPAA does not require that you give your health care provider written permission.  However, your provider may prefer or require that you give written permission.  You may want to ask about your provider’s requirements.

# If my family or friends call my health care provider to ask about my condition, will they have to give my provider proof of who they are?

HIPAA does not require proof of identity in these cases.  However, your health care provider may have his or her own rules for verifying who is on the phone.  You may want to ask your provider about her or his rules.

# Can I have another person pick up my prescription drugs, medical supplies, or x-rays?

Yes. HIPAA allows health care providers (such as pharmacists) to give prescription drugs, medical supplies, X-rays, and other health care items to a family member, friend, or other person you send to pick them up.

Can my health care provider discuss my health information with an interpreter?

Yes.  HIPAA allows your health care provider to share your health information with an interpreter who works for the provider to help communicate with you or your family, friends, or others involved in your care.  If the interpreter is someone who does not work for your health care provider, HIPAA also allows your provider to discuss your health information with the interpreter so long as you do not object.

# How can I help make sure my health care providers share my health information with my family, friends, or others involved in my care or payment for my care when I want them to?

Print a copy of [A Patient's Guide: When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved In Your Care](https://www.hhs.gov/sites/default/files/consumer_ffg.pdf) and discuss it with your health care provider at your next appointment.  You may also want to share this information with your family members, friends, or others involved in your care or payment for your care.

# If the patient is present and has the capacity to make health care decisions, when does HIPAA allow a health care provider to discuss the patient’s health information with the patient’s family, friends, or others involved in the patient’s care or payment for care?

If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient’s health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object.  A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object.  In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient’s care or payment for care.

Here are some examples:

* An emergency room doctor may discuss a patient’s treatment in front of the patient’s friend if the patient asks that her friend come into the treatment room.
* A doctor’s office may discuss a patient’s bill with the patient’s adult daughter who is with the patient at the patient’s medical appointment and has questions about the charges.
* A doctor may discuss the drugs a patient needs to take with the patient’s health aide who has accompanied the patient to a medical appointment.
* A doctor may give information about a patient’s mobility limitations to the patient’s sister who is driving the patient home from the hospital.
* A nurse may discuss a patient’s health status with the patient’s brother if she informs the patient she is going to do so and the patient does not object.

BUT:

* A nurse may not discuss a patient’s condition with the patient’s brother after the patient has stated she does not want her family to know about her condition.

# If the patient is not present or is incapacitated, may a health care provider still share the patient’s health information with family, friends, or others involved in the patient’s care or payment for care?

Yes.  If the patient is not present or is incapacitated, a health care provider may share the patient’s information with family, friends, or others as long as the health care provider determines, based on professional judgment, that it is in the best interest of the patient.  When someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care.  The health care provider may discuss only the information that the person involved needs to know about the patient’s care or payment.

Here are some examples:

* A surgeon who did emergency surgery on a patient may tell the patient’s spouse about the patient’s condition while the patient is unconscious.
* A pharmacist may give a prescription to a patient’s friend who the patient has sent to pick up the prescription.
* A hospital may discuss a patient’s bill with her adult son who calls the hospital with questions about charges to his mother’s account.
* A health care provider may give information regarding a patient’s drug dosage to the patient’s health aide who calls the provider with questions about the particular prescription.

            BUT:

* A nurse may not tell a patient’s friend about a past medical problem that is unrelated to the patient’s current condition.
* A health care provider is not required by HIPAA to share a patient’s information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.

# Does HIPAA require that a health care provider document a patient’s decision to allow the provider to share his or her health information with a family member, friend, or other person involved in the patient’s care or payment for care?

No.  HIPAA does not require that a health care provider document the patient’s agreement or lack of objection.  However, a health care provider is free to obtain or document the patient’s agreement, or lack of objection, in writing, if he or she prefers.  For example, a provider may choose to document a patient’s agreement to share information with a family member with a note in the patient’s medical file.

# May a health care provider discuss a patient’s health information over the phone with the patient’s family, friends, or others involved in the patient’s care or payment for care?

Yes.  Where a health care provider is allowed to share a patient’s health information with a person, information may be shared face-to-face, over the phone, or in writing.

# If a patient’s family member, friend, or other person involved in the patient’s care or payment for care calls a health care provider to ask about the patient’s condition, does HIPAA require the health care provider to obtain proof of who the person is before speaking with them?

No.  If the caller states that he or she is a family member or friend of the patient, or is involved in the patient’s care or payment for care, then HIPAA doesn’t require proof of identity in this case.  However, a health care provider may establish his or her own rules for verifying who is on the phone.  In addition, when someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care.

# Can a patient have a family member, friend, or other person pick up a filled prescription, medical supplies, x-rays, or other similar forms of patient information, for the patient?

Yes.  HIPAA allows health care providers to use professional judgment and experience to decide if it is in the patient’s best interest to allow another person to pick up a prescription, medical supplies, X-rays, or other similar forms of information for the patient.

For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for a patient effectively verifies that he or she is involved in the patient’s care.  HIPAA allows the pharmacist to give the filled prescription to the relative or friend.  The patient does not need to provide the pharmacist with their names in advance.

May a health care provider share a patient’s health information with an interpreter to communicate with the patient or with the patient’s family, friends, or others involved in the patient’s care or payment for care?

Yes.  HIPAA allows covered health care providers to share a patient’s health information with an interpreter without the patient’s written authorization under the following circumstances:

* A health care provider may share information with an interpreter who works for the provider (e.g., a bilingual employee, a contract interpreter on staff, or a volunteer).

For example, an emergency room doctor may share information about an incapacitated patient’s condition with an interpreter on staff who relays the information to the patient’s family.

* A health care provider may share information with an interpreter who is acting on its behalf (but is not a member of the provider’s workforce) if the health care provider has a written contract or other agreement with the interpreter that meets HIPAA’s business associate contract requirements.

For example, many providers are required under Title VI of the Civil Rights Act of 1964 to take reasonable steps to provide meaningful access to persons with limited English proficiency.  These providers often have contracts with private companies, community-based organizations, or telephone interpreter service lines to provide language interpreter services.  These arrangements must comply with the HIPAA business associate agreement requirements at 45 C.F.R. 164.504(e).

* A health care provider may share information with an interpreter who is the patient’s family member, friend, or other person identified by the patient as his or her interpreter, if the patient agrees, or does not object, or the health care provider determines, using his or her professional judgment, that the patient does not object.

For example, health care providers sometimes see patients who speak a certain language and the provider has no employee, volunteer, or contractor who can competently interpret that language.  If the provider is aware of a telephone interpreter service that can help, the provider may have that interpreter tell the patient that the service is available.  If the provider decides, based on professional judgment, that the patient has chosen to continue using the interpreter, the provider may talk to the patient using the interpreter.

# May a health plan disclose protected health information to a person who calls the plan on the beneficiary’s behalf?

### Answer:

Yes, subject to the conditions set forth in [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b) of the HIPAA Privacy Rule. The Privacy Rule at 45 CFR 164.510(b) permits a health plan (or other [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)) to disclose to a family member, relative, or close personal friend of the individual, the protected health information (PHI) directly relevant to that person’s involvement with the individual’s care or payment for care. A covered entity also may make these disclosures to persons who are not family members, relatives, or close personal friends of the individual, provided the covered entity has reasonable assurance that the person has been identified by the individual as being involved in his or her care or payment.

A covered entity only may disclose the relevant PHI to these persons if the individual does not object or the covered entity can reasonably infer from the circumstances that the individual does not object to the disclosure; however, when the individual is not present or is incapacitated, the covered entity can make the disclosure if, in the exercise of professional judgment, it believes the disclosure is in the best interests of the individual.

For example:

* A health plan may disclose relevant PHI to a beneficiary’s daughter who has called to assist her hospitalized, elderly mother in resolving a claims or other payment issue.
* A health plan may disclose relevant PHI to a human resources representative who has called the plan with the beneficiary also on the line, or who could turn the phone over to the beneficiary, who could then confirm for the plan that the representative calling is assisting the beneficiary.
* A health plan may disclose relevant PHI to a Congressional office or staffer that has faxed to the plan a letter or e-mail it received from the beneficiary requesting intervention with respect to a health care claim, which assures the plan that the beneficiary has requested the Congressional office’s assistance.
* A Medicare Part D plan may disclose relevant PHI to a staff person with the Centers for Medicare and Medicaid Services (CMS) who contacts the plan to assist an individual regarding the Part D benefit, if the information offered by the CMS staff person about the individual and the individual’s concerns is sufficient to reasonably satisfy the plan that the individual has requested the CMS staff person’s assistance.

# Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with a person who is not married to the patient or is otherwise not recognized as a relative of the patient under applicable law (e.g., state law)?

Yes. The HIPAA Privacy Rule at [45 CFR 164.510](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-510.xml)(b) permits covered entities to share with an individual’s family member, other relative, close personal friend, or any other person identified by the individual, the information directly relevant to the involvement of that person in the patient’s care or payment for health care. In addition, HIPAA allows a covered entity to disclose information about a patient as necessary to notify, or assist in the notification of (including by helping to identify or locate), such a person of the patient’s location, general condition, or death. In either circumstance, the person can be a patient’s family member, relative, guardian, caregiver, friend, spouse, or partner. The Privacy Rule defers to a covered entity’s professional judgment in these cases and does not require the entity to verify that a person is a family member, friend, or otherwise involved in the patient’s care or payment for care.

HIPAA permits a covered entity to share PHI with anyone from the list of potential recipients, subject to the conditions included at 45 CFR 164.510(b) and described below.  Moreover, the list of potential recipients of PHI under 45 CFR 164.510(b) is in no way limited or impacted by the sex or gender identity of either the patient or the potential recipient.

When making disclosures to the persons listed under 45 CFR 164.510(b), a covered entity should get verbal permission from the patient when possible, or otherwise be able to reasonably infer that the patient does not object to the disclosure, before disclosing information to these persons.  If the patient is incapacitated or not available, a covered entity may share information when, in its professional judgment, doing so is in the patient’s best interest.  Finally, if the individual is deceased, a covered entity may share information with a person who was involved in the individual's care or payment for care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

In contrast to the permitted disclosures described above, there are circumstances in which a covered entity is required to disclose information to a family member or other person involved in an individual’s care. Specifically, in some cases, a spouse, partner, or other person involved in a patient’s care will be the patient’s personal representative and thus generally have the authority to exercise the patient’s rights under the HIPAA Privacy Rule on the patient’s behalf, such as the  right to access medical and other health records as provided at 45 CFR 164.524(a). A covered entity must treat all personal representatives as the individual for purposes of the Privacy Rule, in accordance with 45 CFR 164.502(g).  This means a covered entity may not deny a personal representative, as defined in 45 CFR 164.502(g), the rights afforded to the personal representative under 45 CFR 164.502(g) of the Privacy Rule for any reason, including because of the sex or gender identity of the personal representative. For example, if a state grants legally married spouses health care decision making authority for each other, such that legally married spouses are personal representatives under 45 CFR 164.502(g), the legally married spouse is the patient’s personal representative and a covered entity must provide the spouse access to the patient’s records. In this example, a covered entity that does not provide a patient’s lawful spouse with access because of the sex of the spouses would be in violation of the Privacy Rule.  Similarly, if a person has been granted a legal health care power of attorney for an individual that grants the person the authority to make health care decisions for the individual in a state, that person satisfies the definition of personal representative and a covered entity in that state that denies the person personal representative status because of the gender identity of the person would be in violation of the Privacy Rule.

For more information about HIPAA and Marriage, see [http://www.hhs.gov/hipaa/for-professionals/special-topics/same-sex-marriage/index.html](https://www.hhs.gov/hipaa/for-professionals/special-topics/same-sex-marriage/index.html).” . More general information about when HIPAA permits disclosures to family members, friends, and others involved in a patient’s care or payment for care is available at [http://www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html](https://www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html) (for individuals) and at [http://www.hhs.gov/sites/default/files/provider\_ffg.pdf](https://www.hhs.gov/sites/default/files/provider_ffg.pdf) (for providers).

# What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. See 45 CFR 164.530(c). This means that covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use. See 45 CFR 164.310(d)(2)(i) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

Further, covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member. See 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i). Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers. See 45 CFR 160.103 (definition of “workforce”).

Thus, covered entities are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons. However, the Privacy and Security Rules do not require a particular disposal method. Covered entities must review their own circumstances to determine what steps are reasonable to safeguard PHI through disposal, and develop and implement policies and procedures to carry out those steps. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the form, type, and amount of PHI to be disposed. For instance, the disposal of certain types of PHI such as name, social security number, driver’s license number, debit or credit card number, diagnosis, treatment information, or other sensitive information may warrant more care due to the risk that inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual’s reputation.

In general, examples of proper disposal methods may include, but are not limited to:

* For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
* Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
* For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

For more information on proper disposal of electronic PHI, see the [HHS HIPAA Security Series 3: Security Standards – Physical Safeguards](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf). In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult  [NIST SP 800-88, Guidelines for Media Sanitization.](https://www.hhs.gov/sites/default/files/nistsp800-88-rev1.pdf)

Other methods of disposal also may be appropriate, depending on the circumstances. Covered entities are encouraged to consider the steps that other prudent health care and health information professionals are taking to protect patient privacy in connection with record disposal. In addition, if a covered entity is winding up a business, the covered entity may wish to consider giving patients the opportunity to pick up their records prior to any disposition by the covered entity (and note that many states may impose requirements on covered entities to retain and make available for a limited time, as appropriate, medical records after dissolution of a business).

# May a covered entity dispose of protected health information in dumpsters accessible by the public?

No, unless the protected health information (PHI) has been rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster. In general, a covered entity may not dispose of PHI in paper records, labeled prescription bottles, hospital identification bracelets, PHI on electronic media, or other forms of PHI in dumpsters, recycling bins, garbage cans, or other trash receptacles generally accessible by the public or other unauthorized persons. The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, in any form, including in connection with the disposal of such information. See 45 CFR 164.530(c). In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored. See 45 CFR 164.310(d)(2)(i). Depositing PHI in a trash receptacle generally accessible by the public or other unauthorized persons is not an appropriate privacy or security safeguard. Instead, covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI. Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

For example, depending on the circumstances, proper disposal methods may include (but are not limited to):

* Shredding or otherwise destroying PHI in paper records so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster or other trash receptacle.
* Maintaining PHI for disposal in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
* In justifiable cases, based on the size and the type of the covered entity, and the nature of the PHI, depositing PHI in locked dumpsters that are accessible only by authorized persons, such as appropriate refuse workers.
* For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

For more information on proper disposal of electronic PHI, see the [HHS HIPAA Security Series 3: Security Standards – Physical Safeguards](http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsPhysicalSafeguards.pdf). In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult [NIST SP 800-88, Guidelines for Media Sanitization](https://www.hhs.gov/sites/default/files/nistsp800-88-rev1.pdf).

# May a covered entity hire a business associate to dispose of protected health information?

Yes, a covered entity may, but is not required to, hire a business associate to appropriately dispose of protected health information (PHI) on its behalf. In doing so, the covered entity must enter into a contract or other agreement with the business associate that requires the business associate, among other things, to appropriately safeguard the PHI through disposal. See 45 CFR 164.308(b), 164.314(a), 164.502(e), and 164.504(e). Thus, for example, a covered entity may hire an outside vendor to pick up PHI in paper records or on electronic media from its premises, shred, burn, pulp, or pulverize the PHI, or purge or destroy the electronic media, and deposit the deconstructed material in a landfill or other appropriate area.

# May a covered entity reuse or dispose of computers or other electronic media that store electronic protected health information?

Yes, but only if certain steps have been taken to remove the electronic protected health information (ePHI) stored on the computers or other media before its disposal or reuse, or if the media itself is destroyed before its disposal. The HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of ePHI from electronic media before the media are made available for reuse. See 45 CFR 164.310(d)(2)(i) and (ii). Depending on the circumstances, appropriate methods for removing ePHI from electronic media prior to reuse or disposal may be by clearing (using software or hardware products to overwrite media with non-sensitive data) or purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) the information from the electronic media. If circumstances warrant the destruction of the electronic media prior to disposal, destruction methods may include disintegrating, pulverizing, melting, incinerating, or shredding the media. Covered entities may contract with business associates to perform these services for them.

For more information on proper disposal of ePHI and reuse of electronic media, see the [HHS HIPAA Security Series 3: Security Standards – Physical Safeguards](http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsPhysicalSafeguards.pdf). In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult [NIST SP 800-88, Guidelines for Media Sanitization](https://www.hhs.gov/sites/default/files/nistsp800-88-rev1.pdf).

# How should home health workers or other workforce members of a covered entity dispose of protected health information that they use off of the covered entity’s premises?

The HIPAA Privacy Rule requires that covered entities develop and apply policies and procedures for appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), including through final disposition. See 45 CFR 164.530(c). In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored. See 45 CFR 164.310(d)(2)(i). The Rules are flexible and thus, do not specify particular types of disposal methods; however, covered entities must ensure that the disposal method reasonably protects against impermissible uses and disclosures of PHI and protects against reasonably anticipated threats or hazards to the security of electronic PHI. See 45 CFR 164.530(c)(2) and 164.306(a). Whatever the disposal method, a covered entity must ensure that appropriate workforce members, either working on the premises or off-site, receive training on and follow the disposal policies and procedures of the covered entity. See 45 CFR 164.530(b) and (i), as well as 164.306(a)(4) and 164.308(a)(5) with regard to electronic PHI. These policies and procedures could require, for example, that employees or other workforce members who use PHI off-site, including electronic PHI, return all PHI to the covered entity for appropriate disposal. Or, for example, if appropriate under the circumstances, a covered entity could give off-site workforce members the option of either properly shredding PHI in paper records themselves or returning the PHI to the covered entity for disposal. In cases where workforce members fail to comply with the covered entity’s disposal policies and procedures, the covered entity must apply appropriate sanctions. See 45 CFR 164.530(e).

# Does the HIPAA Privacy Rule require covered entities to keep patients’ medical records for any period of time?

No, the HIPAA Privacy Rule does not include medical record retention requirements. Rather, State laws generally govern how long medical records are to be retained. However, the HIPAA Privacy Rule does require that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other protected health information (PHI) for whatever period such information is maintained by a covered entity, including through disposal. See 45 CFR 164.530(c).

# Are hospitals able to inform the clergy about parishioners in the hospital?

### Answer:

Yes, the HIPAA Privacy Rule allows this communication to occur, as long as the patient has been informed of this use and disclosure, and does not object. The Privacy Rule provides that a hospital or other covered health care provider may maintain in a directory the following information about that individual: the individual’s name; location in the facility; health condition expressed in general terms; and religious affiliation.

The facility may disclose this directory information to members of the clergy. Thus, for example, a hospital may disclose the names of Methodist patients to a Methodist minister unless a patient has restricted such disclosure. Directory information, except for religious affiliation, may be disclosed only to other persons who ask for the individual by name. When, due to emergency circumstances or incapacity, the patient has not been provided an opportunity to agree or object to being included in the facility’s directory, these disclosures may still occur, if such disclosure is consistent with any known prior expressed preference of the individual and the disclosure is in the individual’s best interest as determined in the professional judgment of the provider. See 45 CFR 164.510(a).

# Does the HIPAA Privacy Rule limit an individual’s ability to gather and share family medical history information?

No. The HIPAA Privacy Rule may limit how a covered entity (for example, a health plan or most health care providers) uses or discloses individually identifiable health information, but does not prevent individuals, themselves, from gathering medical information about their family members or from deciding to share this information with family members or others, including their health care providers. Thus, individuals are free to provide their doctors with a complete family medical history or communicate with their doctors about conditions that run in the family.

# Does the HIPAA Privacy Rule limit what a doctor can do with a family medical history?

Yes, if the doctor is a “covered entity” under the HIPAA Privacy Rule. A doctor, who conducts certain financial and administrative transactions electronically, such as electronically billing Medicare or other payers for health care services, is considered a covered health care provider. The HIPAA Privacy Rule limits how a covered health care provider may use or disclose protected health information. The HIPAA Privacy Rule allows a covered health care provider to use or disclose protected health information (other than psychotherapy notes), including family history information, for treatment, payment, and health care operation purposes without obtaining the individual’s written authorization or other agreement. The HIPAA Privacy Rule also generally allows covered entities to disclose protected health information without obtaining the individual’s written authorization or other agreement for certain purposes to benefit the public, for example, circumstances that involve public health research or health oversight activities.

When a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual’s family medical history, this information becomes part of the individual’s medical record and is treated as “protected health information” about the individual. Thus, the individual (and not the family members included in the medical history) may exercise the rights under the HIPAA Privacy Rule to this information in the same fashion as any other information in the medical record, including the right of access, amendment, and the ability to authorize disclosure to others.

Does the HIPAA Privacy Rule apply to an elementary or secondary school?

Generally, no.  In most cases, the *HIPAA* Privacy Rule does not apply to an elementary or secondary school because the school either: (1) is not a *HIPAA* covered entity or (2) is a *HIPAA* covered entity but maintains health information only on students in records that are by definition “education records” under *FERPA* and, therefore, is not subject to the *HIPAA* Privacy Rule.

* *The school is not a HIPAA covered entity.* The *HIPAA* Privacy Rule only applies to health plans, health care clearinghouses, and those health care providers that transmit health information electronically in connection with certain administrative and financial transactions (“covered transactions”). See 45 *CFR* § 160.102.  Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan.  See the definition of “transaction” at 45 *CFR* § 160.103 and 45 *CFR*Part 162, Subparts K–R.  Thus, even though a school employs school nurses, physicians, psychologists, or other health care providers, the school is not generally a *HIPAA* covered entity because the providers do not engage in any of the covered transactions, such as billing a health plan electronically for their services.  It is expected that most elementary and secondary schools fall into this category.
* *The school is a HIPAA covered entity but does not have “protected health information.”* Where a school does employ a health care provider that conducts one or more covered transactions electronically, such as electronically transmitting health care claims to a health plan for payment, the school is a *HIPAA* covered entity and must comply with the *HIPAA* Transactions and Code Sets and Identifier Rules with respect to such transactions.  However, even in this case, many schools would not be required to comply with the *HIPAA* Privacy Rule because the school maintains health information only in student health records that are “education records” under *FERPA* and, thus, not “protected health information” under *HIPAA*.  Because student health information in education records is protected by *FERPA*, the *HIPAA* Privacy Rule excludes such information from its coverage.  See the exception at paragraph (2)(i) to the definition of “protected health information” in the *HIPAA* Privacy Rule at 45 *CFR* § 160.103.  For example, if a public high school employs a health care provider that bills Medicaid electronically for services provided to a student under the *IDEA*, the school is a *HIPAA* covered entity and would be subject to the *HIPAA* requirements concerning transactions.  However, if the school’s provider maintains health information only in what are education records under *FERPA*, the school is not required to comply with the *HIPAA* Privacy Rule.  Rather, the school would have to comply with *FERPA’s* privacy requirements with respect to its education records, including the requirement to obtain parental consent (34 *CFR* § 99.30) in order to disclose to Medicaid billing information about a service provided to a student.

# Does FERPA or HIPAA apply to elementary or secondary school student health records maintained by a health care provider that is not employed by a school?

If a person or entity acting on behalf of a school subject to *FERPA*, such as a school nurse that provides services to students under contract with or otherwise under the direct control of the school, maintains student health records, these records are education records under *FERPA*, just as they would be if the school maintained the records directly.  This is the case regardless of whether the health care is provided to students on school grounds or off-site.  As education records, the information is protected under *FERPA* and not *HIPAA*.

Some outside parties provide services directly to students and are not employed by, under contract to, or otherwise acting on behalf of the school.  In these circumstances, these records are not “education records” subject to *FERPA*, even if the services are provided on school grounds, because the party creating and maintaining the records is not acting on behalf of the school.  For example, the records created by a public health nurse who provides immunization or other health services to students on school grounds or otherwise in connection with school activities but who is not acting on behalf of the school would not be “education records” under *FERPA*.  In such situations, a school that wishes to disclose to this outside party health care provider any personally identifiable information from education records would have to comply with *FERPA* and obtain parental consent.  See 34 *CFR* § 99.30.

With respect to *HIPAA*, even where student health records maintained by a health care provider are not education records protected by *FERPA*, the *HIPAA* Privacy Rule would apply to such records only if the provider conducts one or more of the *HIPAA* transactions electronically, e.g., billing a health plan electronically for his or her services, making the provider a *HIPAA* covered entity.

# Are there circumstances in which the HIPAA Privacy Rule might apply to an elementary or secondary school?

There are some circumstances in which an elementary or secondary school would be subject to the *HIPAA* Privacy Rule, such as where the school is a *HIPAA* covered entity and is not subject to *FERPA*.  As explained previously, most private schools at the elementary and secondary school levels typically do not receive funding from the U.S. Department of Education and, therefore, are not subject to *FERPA*.

A school that is not subject to *FERPA* and is a *HIPAA* covered entity must comply with the *HIPAA*Privacy Rule with respect to any individually identifiable health information it has about students and others to whom it provides health care.  For example, if a private elementary school that is not subject to *FERPA* employs a physician who bills a health plan electronically for the care provided to students (making the school a *HIPAA* covered entity), the school is required to comply with the *HIPAA* Privacy Rule with respect to the individually identifiable health information of its patients.  The only exception would be where the school, despite not being subject to *FERPA*, has education records on one or more students to whom it provides services on behalf of a school or school district that is subject to *FERPA*.  In this exceptional case, the education records of only those publicly-placed students held by the private school would be subject to *FERPA*, while the remaining student health records would be subject to the *HIPAA* Privacy Rule.

# Where the HIPAA Privacy Rule applies, does it allow a health care provider to disclose protected health information (PHI) about a troubled teen to the parents of the teen?

In most cases, yes.  If the teen is a minor, the *HIPAA* Privacy Rule generally allows a covered entity to disclose PHI about the child to the child’s parent, as the minor child’s personal representative, when the disclosure is not inconsistent with state or other law. For more detailed information, see 45 *CFR* § 164.502(g) and the [personal representatives fact sheet](https://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalreps.html).  In some cases, such as when a minor may receive treatment without a parent’s consent under applicable law, the parents are not treated as the minor’s personal representative.  See 45 *CFR* § 164.502(g)(3).  In such cases where the parent is not the personal representative of the teen, other *HIPAA* Privacy Rule provisions may allow the disclosure of PHI about the teen to the parent.  For example, if a provider believes the teen presents a serious danger to self or others, the *HIPAA* Privacy Rule permits a covered entity to disclose PHI to a parent or other person(s) if the covered entity has a good faith belief that:  (1) the disclosure is necessary to prevent or lessen the threat and (2) the parent or other person(s) is reasonably able to prevent or lessen the threat.  The disclosure also must be consistent with applicable law and standards of ethical conduct.  See 45 *CFR* § 164.512(j)(1)(i).

In addition, the Privacy Rule permits covered entities to share information that is directly relevant to the involvement of a family member in the patient’s health care or payment for care if, when given the opportunity, the patient does not object to the disclosure.  Even when the patient is not present or it is impracticable, because of emergency circumstances or the patient’s incapacity, for the covered entity to ask the patient about discussing his or her care or payment with a family member, a covered entity may share this information with the family member when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient.  See 45 *CFR* § 164.510(b).

# Does the HIPAA Privacy Rule allow a health care provider to disclose protected health information (PHI) about a student to a school nurse or physician?

Yes.  The *HIPAA* Privacy Rule allows covered health care providers to disclose PHI about students to school nurses, physicians, or other health care providers for treatment purposes, without the authorization of the student or student’s parent.  For example, a student’s primary care physician may discuss the student’s medication and other health care needs with a school nurse who will administer the student’s medication and provide care to the student while the student is at school. In addition, a covered health care provider may disclose proof of a student's immunizations directly to a school nurse or other person designated by the school to receive immunization records if the school is required by State or other law to have such proof prior to admitting the student, and a parent, guardian, or other person acting *in loco parentis* has agreed to the disclosure.  See 45 CFR 164.512(b)(1)(vi).

# Does FERPA or HIPAA apply to records on students at health clinics run by postsecondary institutions?

*FERPA* applies to most public and private postsecondary institutions and, thus, to the records on students at the campus health clinics of such institutions.  These records will be either education records or treatment records under *FERPA*, both of which are excluded from coverage under the *HIPAA* Privacy Rule, even if the school is a *HIPAA* covered entity.  See the exceptions at paragraphs (2)(i) and (2)(ii) to the definition of “protected health information” at 45 *CFR* § 160.103.

The term “education records” is broadly defined under *FERPA* to mean those records that are:  (1) directly related to a student and (2) maintained by an educational agency or institution or by a party acting for the agency or institution.  See 34 *CFR* § 99.3, “Education records.”

“Treatment records” under *FERPA*, as they are commonly called, are: records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student’s choice.

See 20 *U.S.C.* § 1232g(a)(4)(B)(iv); 34 *CFR* § 99.3, “Education records.”  For example, treatment records would include health or medical records that a university psychologist maintains only in connection with the provision of treatment to an eligible student, and health or medical records that the campus health center or clinic maintains only in connection with the provision of treatment to an eligible student.  (Treatment records also would include health or medical records on an eligible student in high school if the records otherwise meet the above definition.)

“Treatment records” are excluded from the definition of “education records” under *FERPA.*  However, it is important to note, that a school may disclose an eligible student’s treatment records for purposes other than the student’s treatment provided that the records are disclosed under one of the exceptions to written consent under 34 *CFR* § 99.31(a) or with the student’s written consent under 34 *CFR* § 99.30.  If a school discloses an eligible student’s treatment records for purposes other than treatment, the treatment records are no longer excluded from the definition of “education records” and are subject to all other *FERPA* requirements, including the right of the eligible student to inspect and review the records.

While the health records of students at postsecondary institutions may be subject to *FERPA*, if the institution is a *HIPAA* covered entity and provides health care to *non*students, the individually identifiable health information of the clinic’s *non*student patients is subject to the *HIPAA* Privacy Rule.  Thus, for example, postsecondary institutions that are subject to both *HIPAA* and *FERPA* and that operate clinics open to staff, or the public, or both (including family members of students) are required to comply with *FERPA* with respect to the health records of their student patients, and with the *HIPAA* Privacy Rule with respect to the health records of their *non*student patients.

# Does FERPA or HIPAA apply to records on students who are patients at a university hospital?

Patient records maintained by a hospital affiliated with a university that is subject to *FERPA* are not typically “education records” or “treatment records” under *FERPA* because university hospitals generally do not provide health care services to students on behalf of the educational institution. Rather, these hospitals provide such services without regard to the person’s status as a student and not on behalf of a university.  Thus, assuming the hospital is a *HIPAA* covered entity, these records are subject to all of the *HIPAA* rules, including the *HIPAA* Privacy Rule.  However, in a situation where a hospital does run the student health clinic on behalf of a university, the clinic records on students would be subject to *FERPA,* either as “education records” or “treatment records,” and not subject to the *HIPAA* Privacy Rule.

# Where the HIPAA Privacy Rule applies, does it permit a health care provider to disclose protected health information (PHI) about a patient to law enforcement, family members, or others if the provider believes the patient presents a serious danger to self or others?

The *HIPAA* Privacy Rule permits a covered entity to disclose PHI, including psychotherapy notes, when the covered entity has a good faith belief that the disclosure: (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others and (2) is to a person(s) reasonably able to prevent or lessen the threat.  This may include, depending on the circumstances, disclosure to law enforcement, family members, the target of the threat, or others who the covered entity has a good faith belief can mitigate the threat.  The disclosure also must be consistent with applicable law and standards of ethical conduct.  See 45 *CFR* § 164.512(j)(1)(i).  For example, consistent with other law and ethical standards, a mental health provider whose teenage patient has made a credible threat to inflict serious and imminent bodily harm on one or more fellow students may alert law enforcement, a parent or other family member, school administrators or campus police, or others the provider believes may be able to prevent or lessen the chance of harm.  In such cases, the covered entity is presumed to have acted in good faith where its belief is based upon the covered entity’s actual knowledge (i.e., based on the covered entity’s own interaction with the patient) or in reliance on a credible representation by a person with apparent knowledge or authority (i.e., based on a credible report from a family member or other person).  See 45 *CFR* § 164.512(j)(4).

For threats or concerns that do not rise to the level of “serious and imminent,” other *HIPAA* Privacy Rule provisions may apply to permit the disclosure of PHI.  For example, covered entities generally may disclose PHI about a minor child to the minor’s personal representative (e.g., a parent or legal guardian), consistent with state or other laws.  See 45 *CFR* § 164.502(b).

# Are the health records of an individual who is both a student and an employee of a university at which the person receives health care subject to the privacy provisions of FERPA or those of HIPAA?

The individual’s health records would be considered “education records” protected under *FERPA* and, thus, excluded from coverage under the *HIPAA* Privacy Rule.  *FERPA* defines “education records” as records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.  34 *CFR* § 99.3 (“education records”).  While *FERPA*excludes from this definition certain records relating to employees of the educational institution, to fall within this exclusion, such records must, among other things, relate exclusively to the individual in his or her capacity as an employee, such as records that were created in connection with health services that are available only to employees.  Thus, the health or medical records that are maintained by a university as part of its provision of health care to a student who is also an employee of a university are covered by *FERPA* and not the *HIPAA* Privacy Rule.

# Can a postsecondary institution be a “hybrid entity” under the HIPAA Privacy Rule?

Yes.  A postsecondary institution that is a *HIPAA* covered entity may have health information to which the Privacy Rule may apply not only in the health records of nonstudents in the health clinic, but also in records maintained by other components of the institution that are not education records or treatment records under *FERPA*, such as in a law enforcement unit or research department.  In such cases, the institution, as a *HIPAA* covered entity, has the option of becoming a “hybrid entity” and, thus, having the *HIPAA* Privacy Rule apply only to its health care unit.  The school can achieve hybrid entity status by designating the health unit as its “health care component.”  As a hybrid entity, any individually identifiable health information maintained by other components of the university (i.e., outside of the health care component), such as a law enforcement unit, or a research department, would not be subject to the *HIPAA* Privacy Rule, notwithstanding that these components of the institution might maintain records that are not “education records” or treatment records under *FERPA*.

To become a hybrid entity, the covered entity must designate and include in its health care component all components that would meet the definition of a covered entity if those components were separate legal entities. (A covered entity may have more than one health care component.)  However, the hybrid entity is not permitted to include in its health care component other types of components that do not perform the covered functions of the covered entity or components that do not perform support activities for the components performing covered functions.  That is, components that do not perform health plan, health care provider, or health care clearinghouse functions and components that do not perform activities in support of these functions (as would a business associate of a separate legal entity) may not be included in a health care component.  Within the hybrid entity, most of the *HIPAA*Privacy Rule requirements apply only to the health care component, although the hybrid entity retains certain oversight, compliance, and enforcement obligations.  See 45 *CFR* § 164.105 of the Privacy Rule for more information.

# Can a group health plan, or health insurance issuer with respect to a group health plan, disclose to the plan sponsor the protected health information (PHI) required by the Centers for Medicare and Medicaid Services (CMS) for the retiree drug subsidy, without obtaining the individual’s authorization?

Yes, when the conditions set forth in 45 CFR 164.504(f) of the HIPAA Privacy Rule have been met. Specifically, 45 CFR 164.504(f)(3)(i) allows a group health plan or a health insurance issuer with respect to the group health plan – or its business associate – to disclose PHI to a plan sponsor to carry out plan administration functions as long as it meets the requirements of 45 CFR 164.504(f)(2). As such, where the plan sponsor is carrying out the plan administration function of submitting to CMS the PHI required by 42 CFR 423.884 for the retiree drug subsidy, 45 CFR 164.504(f)(2) sets forth how the group health plan’s plan documents are to be amended to allow the group health plan to permit its health insurance issuer (or business associate, such as a third party administrator) to disclose PHI, without the individual’s authorization, to the plan sponsor of the group health plan. As with other disclosures for plan administration functions, the PHI disclosed must be limited to the minimum necessary to fulfill the requirements of 42 CFR 423.884.

# Is a health plan required to periodically notify enrollees about the availability, and how to obtain a copy, of its Notice of Privacy Practices?

### Answer:

Yes. The Privacy Rule requires a health plan to remind enrollees of the availability of its Notice of Privacy Practices, as well as how to obtain a copy, no less frequently than once every 3 years. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c)(1)(ii).

Health plans may satisfy this requirement in a number of ways, including by:

* Sending a copy of their Notice of Privacy Practices.
* Mailing only a reminder concerning the availability of the Notice of Privacy Practices and information on how to obtain a copy.
* Including in a plan-produced newsletter or other publication information about the availability of the Notice of Privacy Practices and how to obtain a copy.

Health plans already may have satisfied the reminder requirement in a number of ways. For instance, a health plan may have adopted the practice of sending its Notice of Privacy Practices to subscribers and enrollees annually. Or, a health plan may have substantially amended its Notice of Privacy Practices recently, and thus, sent the revised Notice to its subscribers and enrollees as required by the Privacy Rule. See 45 CFR 164.520(c)(1)(i)(C). Moreover, a plan may have included information regarding the availability of its Notice of Privacy Practices in annual communications sent to subscribers and enrollees of the plan.

A health plan can satisfy the requirement by providing the reminder notice to the named insured of a policy under which coverage is provided to that named insured and one or more dependents. See 45 CFR 164.520(c)(1)(iii). For instance, if an employee of a firm and her three dependents are covered under a single health plan policy, that health plan can satisfy the reminder requirement by sending information concerning the availability of the Notice of Privacy Practices to just the employee, rather than to the employee and each dependent.

This information is especially timely as the third anniversary of the compliance date of the HIPAA Privacy Rule nears. Health plans, other than small health plans, were first required to distribute their Notice of Privacy Practices to subscribers and enrollees by April 14, 2003. Thus, those health plans that have not already reminded subscribers and enrollees in some manner of the availability of their Notice of Privacy Practices and how they may obtain a copy, must do so no later than April 14, 2006. For small health plans, which had until April 14, 2004, to first distribute their Notices of Privacy Practices, the compliance date for the triennial reminder notice requirement is April 14, 2007. These plans can begin to prepare now to meet this requirement using the most efficient means, such as including the reminder notice of the availability of the Notice of Privacy Practices in open enrollment materials, a group health plan newsletter provided to all members, or similar all-member mailings.

# What is a covered entity's liability under the HIPAA Privacy Rule for sharing data inappropriately to or through a health information organization (HIO) or other electronic health information exchange network?

A covered entity that exchanges protected health information (PHI) to or through a HIO or otherwise participates in electronic health information exchange is responsible for its own non-compliance with the Privacy Rule, and for violations by its workforce. A covered entity is not directly liable for a violation of the Privacy Rule by a HIO acting as its business associate, if an appropriate business associate agreement is in place. Nor can a HIO as a business associate be held liable for civil money penalties arising from violations of the Privacy Rule. Rather, where a business associate agreement exists between a covered entity and a HIO for the electronic exchange of PHI, the HIO will be contractually obligated to adequately safeguard the PHI and to report noncompliance with the agreement terms to the covered entity, and the covered entity will be held accountable for taking appropriate action to cure known noncompliance by the business associate, and if unable to do so, to terminate the business associate relationship. See 45 C.F.R. §§ 164.502(e), 164.504(e). Furthermore, a covered entity is not liable for a disclosure that is based on the non-compliance of another entity within the health information exchange, as long as the covered entity has complied with the Privacy Rule.

# Does the HIPAA Privacy Rule require a covered entity to “police” a health information organization (HIO), which functions as its business associate?

No. As with other business associates, the Privacy Rule would require that a covered entity enter into a relationship with a HIO in a way which anticipates and reasonably safeguards against the potential for inappropriate uses and disclosures, specifically through the use of a business associate agreement. The Privacy Rule also would require the covered entity to respond appropriately to complaints and evidence of violations, but it would not otherwise require the covered entity to actively monitor or oversee the extent to which a HIO, acting as its business associate, abides by the privacy provisions of the agreement, or the means by which the HIO carries out its privacy safeguard obligations. See 45 C.F.R. §§ 164.502(e), 164.504(e).

How should a covered entity respond to any HIPAA Privacy Rule violation of a health information organization (HIO) acting as its business associate?

The Privacy Rule establishes a series of steps a covered entity should take in response to any complaints or other evidence it receives that a HIO has violated its business associate agreement, which include the following:

* investigation of any complaint received, as well as of other information containing credible evidence of a violation;
* reasonable steps to cure/end any material breaches or violations it becomes aware of;
* termination of the agreement where attempts to cure a material breach are unsuccessful; and
* in the event termination of the agreement is not feasible, the report of violation(s) to the Secretary of HHS, through OCR. See 45 C.F.R. § 164.504(e).

# Who is liable under the HIPAA Privacy Rule where multiple covered entities have signed on to a single business associate agreement and one member breaches the agreement?

The Privacy Rule is flexible enough to allow multiple covered entities to exchange information with each other in an electronically networked environment upon entering into a single, multi-party business associate agreement. Regardless of the number of signatories, the obligations in a multi-party business associate agreement will be largely bi-directional. Covered entities will still be accountable for the actions of their workforce, as well as the contents and enforcement of its business associate agreement with the health information organization (HIO). See 45 C.F.R. §§ 164.530(b),(e) and 164.504(e). Covered entities will not be liable, however, for the violations of other participants in the HIO’s health information exchange.

# May a covered health care provider disclose electronic protected health information (PHI) through a health information organization (HIO) to another health care provider for treatment?

Yes. The Privacy Rule permits a covered entity to disclose PHI to another health care provider for treatment purposes. See 45 C.F.R. § 164.506. Further, a covered entity may use a HIO to facilitate the exchange of such information for treatment purposes, provided it has a business associate agreement with the HIO that requires the HIO to protect the information. See 45 C.F.R. §§ 164.502(e), 164.504(e).

# May a health information organization (HIO) manage a master patient index on behalf of multiple HIPAA covered entities?

Yes. A HIO may receive protected health information from multiple covered entities, and manage, as a business associate on their behalf, a master patient index for purposes of identifying and linking all information about a particular individual. Disclosures to, and use of, a HIO for such purposes is permitted as part of the participating covered entities’ health care operations under the HIPAA Privacy Rule, to the extent the purpose of the master patient index is to facilitate the exchange of health information by those covered entities for purposes otherwise permitted by the Privacy Rule, such as treatment.

# What may a HIPAA covered entity’s business associate agreement authorize a health information organization (HIO) to do with electronic protected health information (PHI) it maintains or has access to in the network?

A business associate agreement may authorize a business associate to make uses and disclosures of PHI the covered entity itself is permitted by the HIPAA Privacy Rule to make. See 45 C.F.R. § 164.504(e). In addition, the Privacy Rule permits a business associate agreement to authorize a business associate (e.g., a HIO) to: (1) use and disclose PHI for the proper management and administration of the business associate, in accordance with 45 C.F.R. § 164.504(e)(4); and (2) to provide data aggregation services related to the health care operations of the covered entities for which it has agreements. In most cases, the permitted uses and disclosures established by a business associate agreement will vary based on the particular functions or services the business associate is to provide the covered entity. Similarly, a covered entity’s business associate agreement with a HIO will vary depending on a number of factors, such as the electronic health information exchange purpose which the HIO is to manage, the particular functions or services the HIO is to perform for the covered entity, and any other legal obligations a HIO may have with respect to the PHI. For example, the business associate agreements between covered entities and a HIO may authorize the HIO to:

•Manage authorized requests for, and disclosures of, PHI among participants in the network;
•Create and maintain a master patient index;
•Provide a record locater or patient matching service;
•Standardize data formats;
•Implement business rules to assist in the automation of data exchange;
•Facilitate the identification and correction of errors in health information records; and
•Aggregate data on behalf of multiple covered entities.

# May a health information organization (HIO), acting as a business associate of a HIPAA covered entity, de-identify information and then use it for its own purposes?

A HIO, as a business associate, may only use or disclose protected health information (PHI) as authorized by its business associate agreement with the covered entity. See 45 C.F.R. § 164.504(e). The process of de-identifying PHI constitutes a use of PHI. Thus, a HIO may only de-identify PHI it has on behalf of a covered entity to the extent that the business associate agreement authorizes the HIO to do so. However, once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and, thus, may be used and disclosed by the covered entity or HIO for any purpose (subject to any other applicable laws).

# How may the HIPAA Privacy Rule’s minimum necessary standard apply to electronic health information exchange through a networked environment?

The Privacy Rule generally requires covered entities to take reasonable steps to limit uses, disclosures, or requests (if the request is to another covered entity) of protected health information (PHI) to the minimum necessary to accomplish the intended purpose. However, in some cases, the Privacy Rule does not require that the minimum necessary standard be applied, such as, for example, to disclosures to or requests by a health care provider for treatment purposes, or to disclosures to the individual who is the subject of the information. For routine requests and disclosures, standard protocols may be used to apply the minimum necessary standard, and individual review of each request or disclosure is not required. For non-routine requests and disclosures, the Privacy Rule requires that criteria be developed for purposes of applying the minimum necessary standard on an individual basis to each request or disclosure. For requests for PHI by another covered entity, the disclosing covered entity may rely, if reasonable under the circumstances, on the requested disclosure as the minimum necessary. See 45 C.F.R. §§ 164.502(b), 164.514(d).

Depending on the type of request or disclosure, it may be that some or many of the requests or disclosures to or through the health information organization (HIO) by a covered entity may not be subject to the Privacy Rule’s minimum necessary standard. This would be true in the case of a HIO whose primary purpose is to exchange electronic PHI between and among several hospitals, doctors, pharmacies, and other health care providers for treatment. However, even though the Privacy Rule does not require that the minimum necessary standard be applied to electronic health information exchanges for treatment purposes, the covered entities participating in the electronic networked environment and the HIO are free to apply the concepts of the minimum necessary standard to develop policies that limit the information they include and exchange, even for treatment purposes. For electronic health information exchanges by a covered entity to and through a HIO that are subject to the minimum necessary standard, such as for a payment or health care operations purpose, the Privacy Rule would require that the minimum necessary standard be applied to that exchange and that the business associate agreement limit the HIO’s disclosures of, and requests for, PHI accordingly. However, as one covered entity may rely, if reasonable, on another covered entity’s request as being the minimum necessary amount of PHI, the HIO’s business associate agreement similarly can authorize and instruct the HIO to rely on the requests of covered entities as the minimum necessary, where appropriate, to help facilitate disclosures between covered entities.

When the minimum necessary standard is required by the Privacy Rule, or the policies of the HIO and participating covered entities, to be applied to certain exchanges of electronic health information, the application of the minimum necessary standard can be automated by the HIO for routine disclosures and requests through the use of standard protocols, business rules, and standardization of data. More complex or non-routine disclosures and requests may not lend themselves to automation, and may require individual review under the Privacy Rule, to the extent the Privacy Rule otherwise applied to the disclosure or request.

# Does the HIPAA Privacy Rule permit a covered entity to disclose psychotherapy notes to or through a health information organization (HIO)?

Yes, provided the covered entity has obtained the individual’s written authorization in accordance with 45 C.F.R. § 164.508. See 45 C.F.R. § 164.501 for the definition of “psychotherapy notes.” With few exceptions, the Privacy Rule requires a covered entity to obtain individual authorization prior to a disclosure of psychotherapy notes, even for a disclosure to a health care provider other than the originator of the notes for treatment purposes. For covered entities operating in an electronic environment, the Privacy Rule does, however, allow covered entities to disclose protected health information pursuant to an electronic copy of a valid and signed authorization, as well as to obtain HIPAA authorizations electronically from individuals, provided any electronic signature is valid under applicable law.

# To what extent does the HIPAA Privacy Rule allow third parties to access protected health information (PHI) through a health information organization (HIO) for purposes other than treatment, payment, and health care operations?

The Privacy Rule would permit a HIO, acting as a business associate of one or more covered entities, to make any disclosure the covered entities are permitted by the Privacy Rule to make, provided the HIO’s business associate agreement(s) authorizes the disclosure. See 45 C.F.R. § 164.504(e). For example, the Privacy Rule permits a covered entity to make disclosures of PHI for public health and research purposes, provided certain conditions are met. Such disclosures may be made by a HIO, on behalf of one or more covered entities, provided the covered entities or HIO satisfy all of the Privacy Rule’s applicable conditions, and the business associate agreement(s) with the HIO authorize the HIO to make the disclosure.

# Who is responsible for amendment of protected health information in an electronic health information exchange environment?

The HIPAA Privacy Rule designates a covered entity as the responsible party for acting on an amendment request. However, a health information organization (HIO), acting as a business associate of the covered entity, may be required by its business associate contract to perform certain functions related to amendments, such as informing other participants in the HIO’s health information exchange who are known to have the individual’s information, of the amendment. See 45 C.F.R. § 164.504(e)(2)(i)(F).

# What are a covered entity’s responsibilities to notify others in a network if an amendment to protected health information is made?

Under the HIPAA Privacy Rule, a covered entity must make reasonable efforts to communicate an amendment to others in the network identified by the individual as needing the amendment, as well as generally to other parties that are known to have the information about the individual. It is also the entity’s responsibility to communicate the amendment within a reasonable timeframe. A health information organization (HIO), with the ability to track where information was exchanged in the past, or to otherwise identify where an individual’s information resides on the network, can assist the covered entity, as its business associate, in efficiently disseminating amended information to appropriate recipients throughout the electronic network.

# In an electronic health information exchange environment, what is a designated record set for purposes of an individual’s right of access under the HIPAA Privacy Rule?

To the extent covered entities maintain their own electronic records systems, their choice to link those systems to a network for electronic health information exchange purposes would not necessarily change the status of information maintained within their designated record sets. That is, information that meets the definition of a designated record set remains part of the designated record set even if that information is linked to a network. See 45 C.F.R. § 164.501 (definition of “designated record set”). Covered entities should be aware, however, that whatever information they import into their electronic records via a network may become an integrated part of their designated record set(s). Network participation alone, however, would not make all other information about the individual that is accessible through the network part of a covered entity’s designated record set. Thus, the ability to link to information through a network does not obligate a covered entity to provide access to the designated record set of another entity participating in the network.

# How would a covered entity or health information organization (HIO), acting on its behalf, know if someone were a personal representative for the purpose of granting access under the HIPAA Privacy Rule?

The Privacy Rule’s verification standard requires that covered entities develop and implement reasonable policies and procedures to verify the identity and authority of such persons, if otherwise unknown to them, before granting them access to protected health information (PHI). See 45 C.F.R. § 164.514(h). Once verified, the personal representative can then be given the appropriate credentials for authentication and access through an electronic system. The Privacy Rule allows covered entities to rely on their professional judgment, as well as industry standards, in designing reasonable verification and authentication processes.
The Privacy Rule permits a covered entity to assign this function to a HIO, acting as its business associate, so long as the relevant standards are complied with. For example, a covered entity could use the HIO to assign the appropriate credentials and authenticate personal representatives, and any others, seeking access to PHI.

# How may judgments be made electronically about denial of access under the HIPAA Privacy Rule?

The Privacy Rule differentiates between two types of denial, reviewable and unreviewable. See 45 C.F.R. § 164.524(a)(2), (3). As to the unreviewable grounds for denial, there are essentially two decisions a covered entity will need to make with respect to electronic access: 1) whether it may deny access based on one or more of the grounds identified by the Privacy Rule; and 2) how to implement such decisions categorically in the electronic environment.

A covered entity may decide, for example, to categorically deny access to certain types of information to which no access right exists, such as psychotherapy notes. The Privacy Rule would permit denial without review, and a case-by-case judgment would not be necessary. Similarly, the covered entity may make such a system-wide decision with respect to other types of protected health information where the Privacy Rule permits an unreviewable denial of access.

In contrast, reviewable grounds for denial of access require decisions be made on a case-by-case basis through the professional judgment of licensed health care providers. Professional judgment also would be required if individuals exercise their right to appeal a denial of access made on reviewable grounds. As computer logic cannot be a substitute for professional judgment in these cases, these types of activities cannot be carried out categorically or in an automated way. Neither could these decisions be delegated to a health information organization (HIO), unless a licensed health care professional at the HIO were assigned the task of making the access determinations.

# Does the HIPAA Privacy Rule inhibit electronic health information exchange across different states or jurisdictions?

No. The Privacy Rule establishes a federal baseline of privacy protections and rights, which applies to covered entities consistently across state borders. The Privacy Rule, however, as required by HIPAA, does not preempt State laws that provide greater privacy protections and rights. Thus, as with covered entities that conduct business today on paper in a multi-jurisdictional environment, covered entities participating in electronic health information exchange need to be cognizant of States with more stringent privacy laws that will affect the exchange of electronic health information across State lines. In addition, other Federal laws also may apply more stringent or different requirements to such exchanges depending on the circumstances. Covered entities and health information organizations (acting as their business associates) which participate in multi-jurisdictional electronic health information exchange should establish privacy policies for the network that accommodate these variances.

# How do HIPAA authorizations apply to an electronic health information exchange environment?

The HIPAA Privacy Rule requires the individual’s written authorization for any use or disclosure of protected health information (PHI) not otherwise expressly permitted or required by the Privacy Rule. For example, authorizations are not generally required to disclose PHI for treatment, payment, or health care operations purposes because covered entities are permitted to use and disclose PHI for such purposes, with few exceptions. Thus, to the extent the primary purpose of any electronic health information exchange is to exchange clinical information among health care providers for treatment, HIPAA authorizations are unlikely to be a common method of effectuating individual choice for the exchange. However, if the purpose of a covered entity sharing PHI through a health information organization is for a purpose not otherwise permitted by the Privacy Rule, then a HIPAA authorization would be required. In such cases, the Privacy Rule would allow covered entities to disclose PHI pursuant to an electronic copy of a valid and signed authorization. Further, the Privacy Rule allows HIPAA authorizations to be obtained electronically from individuals, provided any electronic signature is valid under applicable law.

# Can a covered entity use existing aspects of the HIPAA Privacy Rule to give individuals the right to Opt-In or Opt-Out of electronic health information exchange?

Yes. In particular, the Privacy Rule’s provisions for optional consent and the right to request restrictions can support and facilitate individual choice with respect to the electronic exchange of health information through a networked environment, depending on the purposes of the exchange. The Privacy Rule allows covered entities to obtain the individual’s consent in order to use or disclose protected health information (PHI) for treatment, payment, and health care operations purposes. If a covered entity chooses to obtain consent, the Privacy Rule provides the covered entity with complete flexibility as to the content and manner of obtaining the consent. 45 C.F.R. § 164.506(b). Similarly, the Privacy Rule also provides individuals with a right to request that a covered entity restrict uses or disclosures of PHI about the individual for treatment, payment, or health care operations purposes. See 45 C.F.R. § 164.522(a). While covered entities are not required to agree to an individual’s request for a restriction, they are required to have policies in place by which to accept or deny such requests. Thus, covered entities may use either the Privacy Rule’s provisions for consent or right to request restrictions to facilitate individual choice with respect to electronic health information exchange.

Further, given the Privacy Rule’s flexibility, covered entities could design processes that apply on a more global level (e.g., by requiring an individual’s consent prior to making any disclosure of PHI to or through a health information organization (HIO), or granting restrictions only in which none of the individual’s information is to be exchanged to or through the HIO) or at a more granular level (such as by type of information, potential recipients, or the purposes for which a disclosure may be made). Whatever the policy, such decisions may be implemented on an organization-wide level, or across a HIO’s health information exchange (such as based on the consensus of the health information exchange participants).

# Who has the right to consent or the right to request restrictions with respect to whether a covered entity may electronically exchange a minor’s protected health information to or through a health information organization (HIO)?

As with a minor’s paper medical record, generally a parent, guardian, or other person acting in loco parentis with legal authority to make health care decisions on behalf of the minor is the personal representative of the minor under the HIPAA Privacy Rule and, thus, is able to exercise all of the HIPAA rights with respect to the minor’s health information. Thus, a parent, guardian, or other person acting in loco parentis who is a personal representative would be able to consent to, if the covered entity has adopted a consent process under the Privacy Rule, or to request restrictions on, disclosures of the minor’s health information to or through a HIO for treatment or other certain purposes. However, there are a few exceptions when the parent, guardian, or other person acting in loco parentis is not the personal representative of the minor child, such as:

(1) when State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service;

(2) when a court determines or other law authorizes someone other than the parent, guardian, or person acting in loco parentis to make treatment decisions for a minor; and

(3) when a parent, guardian, or person acting in loco parentis agrees to a confidential relationship between the minor and a health care provider. In such cases, it is only the minor, and not the parent(s), who may exercise the HIPAA rights with respect to the minor’s health information.

# Can a covered entity use existing aspects of the HIPAA Privacy Rule to give individuals the right to decide whether sensitive information about them may be disclosed to or through a health information organization (HIO)?

Yes. To the extent a covered entity is using a process either to obtain consent or act on an individual’s right to request restrictions under the Privacy Rule as a method for effectuating individual choice, policies can be developed for obtaining consent or honoring restrictions on a granular level, based on the type of information involved. For example, specific consent and restriction policies could be developed, either on an organization level or HIO level, for HIV/AIDS, mental health, genetic, and/or substance abuse information. In addition, there may be other Federal and State laws that will affect a covered entity’s exchange of this sensitive information to or through a HIO, and covered entities should consider these other laws when developing individual choice policies. For example, such laws may prescribe the form of consent that is required or create other requirements for the disclosure of information based on the type of information or the intended recipient.

# Does the HIPAA Privacy Rule permit a covered entity to disclose psychotherapy notes to or through a health information organization (HIO)?

Yes, provided the covered entity has obtained the individual’s written authorization in accordance with 45 C.F.R. § 164.508. See 45 C.F.R. § 164.501 for the definition of “psychotherapy notes.” With few exceptions, the Privacy Rule requires a covered entity to obtain individual authorization prior to a disclosure of psychotherapy notes, even for a disclosure to a health care provider other than the originator of the notes, for treatment purposes. For covered entities operating in an electronic environment, the Privacy Rule does, however, allow covered entities to disclose protected health information pursuant to an electronic copy of a valid and signed authorization, as well as to obtain HIPAA authorizations electronically from individuals, provided any electronic signature is valid under applicable law.

# Is a health information organization (HIO) covered by the HIPAA Privacy Rule?

Generally, no. The HIPAA Privacy Rule applies to health plans, health care clearinghouses, and health care providers that conduct covered transactions. The functions a HIO typically performs do not make it a health plan, health care clearinghouse, or covered health care provider. Thus, a HIO is generally not a HIPAA covered entity. However, a HIO that performs certain functions or activities on behalf of, or provides certain services to, a covered entity which require access to PHI would be a business associate under the Privacy Rule. See 45 C.F.R. § 160.103 (definition of “business associate”). HIPAA covered entities must enter into contracts or other agreements with their business associates that require the business associates to safeguard and appropriately protect the privacy of protected health information. See 45 C.F.R. §§ 164.502(e), 164.504(e). (See also the relevant business associate requirements in the HIPAA Security Rule at 45 C.F.R. §§ 164.308(b), 164.314(a).) For instance, a HIO that manages the exchange of PHI through a network on behalf of multiple covered health care providers is a business associate of the covered providers, and thus, one or more business associate agreements would need to be in place between the covered providers and the HIO.

# Can a health information organization (HIO) operate as a business associate of multiple covered entities participating in a networked environment?

Yes. A HIO can operate as a business associate of multiple covered entities participating in a networked environment. The HIPAA Privacy Rule does not prohibit an entity from acting as a business associate of multiple covered entities and performing functions or activities that involve access to protected health information for the collective benefit of the covered entities. In addition, the Privacy Rule would not require separate business associate agreements between each of the covered entities and the business associate. Rather, the Privacy Rule would permit the covered entities participating in a networked environment and the HIO to operate under a single business associate agreement that was executed by all participating covered entities and the common business associate.

# What are some considerations in developing and implementing a business associate agreement with a health information organization (HIO)?

In general, the HIPAA Privacy Rule requires that the contract between a covered entity and its business associate establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate, but provides that the contract may not authorize the business associate to use or disclose PHI in a manner that would violate the Privacy Rule. In addition, the contract must require the business associate to appropriately safeguard PHI. See 45 C.F.R. § 164.504(e). See also the relevant business associate requirements of the HIPAA Security Rule at 45 C.F.R. § 164.314(a). Given these required elements of a business associate agreement, covered entities participating in a networked environment with a HIO can use the business associate agreement as a tool to help shape the specific terms and conditions of the information exchange the HIO will manage, as well as the safeguards that will be in place to ensure information is protected and only shared appropriately.

While a business associate contract technically can authorize the business associate to make any number of uses and disclosures permitted under the Privacy Rule, the parties can, and likely would want to, further restrict in the contract what the HIO can and will do with PHI. Defining the permitted uses and disclosures by the HIO may depend on a number of factors, including the purposes of the information exchange through the network (e.g., for treatment purposes), how individual preferences and choice will be honored, as applicable, and any other legal obligations on covered entities and/or HIOs with respect to the PHI in the network. For instance, if the HIO will primarily manage the exchange of PHI among participating entities for treatment purposes, then the parties should, in the business associate agreement, define the HIO’s permitted uses and disclosures of PHI with those limited purposes in mind.

# Can a health information organization (HIO), as a business associate, exchange protected health information (PHI) with another HIO acting as a business associate?

Yes, so long as the disclosure of PHI is authorized by the HIO’s business associate agreement and the information exchange would be permitted by the HIPAA Privacy Rule. For example, a HIO may disclose, on behalf of a primary care physician, PHI about an individual for treatment purposes in response to a query from another HIO, acting on behalf of a hospital at which the individual is a patient, unless, for instance, the primary care physician has agreed to the patient’s request to restrict such disclosures. Similarly, a HIO that is a business associate of two different covered entities may share PHI it receives from one covered entity with the other covered entity as permitted by the Privacy Rule and its business associate agreement, for example, for treatment purposes, subject to any applicable restrictions.

# Can a health information organization (HIO) participate as part of an organized health care arrangement (OHCA)?

A HIO, by definition, cannot participate as part of an OHCA because the HIPAA Privacy Rule defines OHCA as an arrangement involving only health care providers or health plans, neither of which a HIO qualifies as. However, a HIO may be a business associate of an OHCA if the HIO performs functions or activities on behalf of the OHCA. See 45 C.F.R. § 160.103 (definitions of “organized health care arrangement” and “business associate”). For example, a hospital and the health care providers with staff privileges at the hospital are an OHCA for purposes of the Privacy Rule. To the extent such an arrangement uses a HIO for electronic health information exchange, the HIO would be a business associate of the OHCA.

# Can a health information organization (HIO) participate as part of an affiliated covered entity?

A HIO generally is not a HIPAA covered entity and the HIPAA Privacy Rule allows only certain legally separate covered entities to designate themselves as a single affiliated covered entity for purposes of complying with the Privacy Rule. Thus, a HIO generally may not participate as part of an affiliated covered entity. See 45 C.F.R. § 164.105(b) for the requirements and conditions regarding affiliated covered entities.

# May a HIPAA Notice of Privacy Practices (NPP) specifically mention that protected health information (PHI) will be disclosed to and through a health information organization (HIO)? May the NPP mention that the covered health care provider uses an electronic health record (EHR)?

Yes, covered entities are permitted to include such information in their NPPs. The HIPAA Privacy Rule requires that a covered entity’s NPP describe the types of uses and disclosures of PHI a covered entity is permitted to make. The Rule also requires that a covered entity’s NPP include at least one example of the uses and disclosures the covered entity is permitted to make for treatment, payment, and health care operations purposes. See 45 C.F.R. § 164.520(b).  While the Privacy Rule does not require that these examples describe the covered entity’s disclosure of PHI to and through a HIO for treatment and other purposes, or that a covered health care provider uses an EHR, the Privacy Rule does not preclude a covered entity from including in its NPP additional information concerning the covered entity’s participation in these activities. Alternatively, a covered entity may wish to provide the individual with a separate notice of the disclosures that may be made to and through a HIO, and how the individual’s health information will be protected.
Such notice that mentions that PHI will be disclosed to and through a HIO or that the covered health care provider uses an EHR would help facilitate the openness and transparency in electronic health information exchange that is important for building trust and thus, is encouraged. Some individuals also may find the fact that a health care provider participates in electronic health information exchange, or that the provider uses an EHR, to be an important factor that could lead individuals to choose that provider over another. Also, to the extent the individual is provided with certain choices of how or if the individual’s information is to be exchanged through a HIO, notice of the disclosures a covered entity may make to and through a HIO, as well as how the individual’s information will be protected, would be an important element of informing such choices.

# Are health information organizations (HIOs) required to have a HIPAA Notice of Privacy Practices (NPP)?

Generally, no. The HIPAA Privacy Rule’s NPP obligations extend only to HIPAA covered entities and the functions a HIO generally performs do not make it a HIPAA covered entity (i.e., a health plan, health care clearinghouse, or covered health care provider). See 45 C.F.R. § 160.103 (definition of “covered entity”). However, while a HIO does not itself have a HIPAA obligation to provide a NPP to individuals, the Privacy Rule permits covered entities that participate in electronic health information exchange with the HIO to provide notice to individuals of the disclosures that will be made to and through the HIO and through the network, as well as how individuals’ health information will be protected by the HIO.

# May covered entities that operate in electronic environments provide individuals with their HIPAA Notice of Privacy Practices (NPP) electronically?

Yes, provided the individual agrees to receive the covered entity’s NPP electronically and such agreement has not been withdrawn (although the individual always retains the right to receive a paper copy of the NPP upon request). Further, where health care is delivered to an individual electronically, such as through e-mail, or over the Internet, the provider must send an electronic NPP automatically and contemporaneously in response to the individual’s request for service. Except in an emergency treatment situation, a covered entity that has a direct treatment relationship with an individual and who delivers an NPP electronically also must make a good faith effort to obtain a written acknowledgment of receipt, either electronically or through other means. In addition, the HIPAA Privacy Rule requires a covered entity that maintains a website providing information about the covered entity’s services or benefits to prominently post its NPP on its website. See 45 C.F.R. § 164.520(c).

# Does the HIPAA Privacy Rule permit a covered health care provider to e-mail or otherwise electronically exchange protected health information (PHI) with another provider for treatment purposes?

Yes. The Privacy Rule allows covered health care providers to share PHI electronically (or in any other form) for treatment purposes, as long as they apply reasonable safeguards when doing so. Thus, for example, a physician may consult with another physician by e-mail about a patient’s condition, or health care providers may electronically exchange PHI to and through a health information organization (HIO) for patient care.

How may the HIPAA Privacy Rule’s requirements for verification of identity and authority be met in an electronic health information exchange environment?

The Privacy Rule requires covered entities to verify the identity and authority of a person requesting protected health information (PHI), if not known to the covered entity. See 45 C.F.R. § 164.514(h). The Privacy Rule allows for verification in most instances in either oral or written form, although verification does require written documentation when such documentation is a condition of the disclosure.
The Privacy Rule generally does not include specific or technical verification requirements and thus, can flexibly be applied to an electronic health information exchange environment in a manner that best supports the needs of the exchange participants and the health information organization (HIO). For example, in an electronic health information exchange environment:

* Participants can agree by contract or otherwise to keep current and provide to the HIO a list of authorized persons so the HIO can appropriately authenticate each user of the network.
* For persons claiming to be government officials, proof of government status may be provided by having a legitimate government e-mail extension (e.g., xxx.gov).
* Documentation required for certain uses and disclosures may be provided in electronic form, such as scanned images or pdf files.
* Documentation requiring signatures may be provided as a scanned image of the signed documentation or as an electronic document with an electronic signature, to the extent the electronic signature is valid under applicable law.

# Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C.

Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual’s request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted e-mail is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.

Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

**Does the HIPAA Privacy Rule allow covered entities participating in electronic health information exchange with a health information organization (HIO) to establish a common set of safeguards?**

Yes. The Privacy Rule requires a covered entity to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), including reasonable safeguards to protect against any intentional or unintentional use or disclosure in violation of the Privacy Rule. See 45 C.F.R. § 164.530(c). Each covered entity can evaluate its own business functions and needs, the types and amounts of PHI it collects, uses, and discloses, size, and business risks to determine adequate safeguards for its particular circumstances.

With respect to electronic health information exchange, the Privacy Rule would allow covered entities participating in an exchange with a HIO to agree on a common set of privacy safeguards that are appropriate to the risks associated with exchanging PHI to and through the HIO. In addition, as a requirement of participation in the electronic health information exchange with the HIO, these commonly agreed to safeguards also could be extended to other participants, even if they are not covered entities. A common or consistent set of standards applied to the HIO and its participants may help not only to facilitate the efficient exchange of information, but also to foster trust among both participants and individuals.

# Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

### Answer:

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers’ primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

* Health care staff may orally coordinate services at hospital nursing stations.
* Nurses or other health care professionals may discuss a patient’s condition over the phone with the patient, a provider, or a family member.
* A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
* A physician may discuss a patients’ condition or treatment regimen in the patient’s semi-private room.
* Health care professionals may discuss a patient’s condition during training rounds in an academic or training institution.
* A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

# May physician's offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

### Answer

Yes. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html), such as physician’s offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(a)(1)(iii).

# Are physicians and doctor's offices prohibited from maintaining patient medical charts at bedside or outside of exam rooms, or from engaging in other customary practices where the potential exists for patient information to be incidentally disclosed to others?

### Answer:

No. The HIPAA Privacy Rule does not prohibit [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual’s privacy while engaging in these practices. Covered entities must implement reasonable safeguards to protect an individual’s privacy. In addition, covered entities must reasonably restrict how much information is used and disclosed, where appropriate, as well as who within the entity has access to protected health information. Covered entities must evaluate what measures make sense in their environment and tailor their practices and safeguards to their particular circumstances.

For example, the Privacy Rule does not prohibit covered entities from engaging in the following practices, where reasonable precautions have been taken to protect an individual’s privacy:

* Maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., “high fall risk” or “diabetic diet”) at patient bedside or at the doors of hospital rooms.

**Possible safeguards may include:** reasonably limiting access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by.
* Announcing patient names and other information over a facility’s public announcement system.

**Possible safeguards may include:** limiting the information disclosed over the system, such as referring the patients to a reception desk where they can receive further instructions in a more confidential manner.
* Use of X-ray lightboards or in-patient logs, such as whiteboards, at a nursing station.

**Possible safeguards may include:** if the X-ray lightboard is in an area generally not accessible by the public, or if the nursing station whiteboard is not readily visible to the public, or any other safeguard which reasonably limits incidental disclosures to the general public.

The above examples of possible safeguards are not intended to be exclusive. Covered entities may engage in any practice that reasonably safeguards protected health information to limit incidental uses and disclosures.

# A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the HIPAA Privacy Rule allow the clinic to continue this practice?

### Answer:

Yes, the Privacy Rule permits this practice as long as the clinic takes reasonable and appropriate measures to protect the patient’s privacy. The physician or other health care professionals use the patient charts for treatment purposes. Incidental disclosures to others that might occur as a result of the charts being left in the box are permitted, if the minimum necessary and reasonable safeguards requirements are met. [See our section on Incidental Uses and Disclosures](https://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html). As the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to the examination, the minimum necessary requirement would be satisfied.

Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by. Each covered entity must evaluate what measures are reasonable and appropriate in its environment. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may tailor measures to their particular circumstances. See 45 CFR 164.530(c).

# A hospital customarily displays patients' names next to the door of the hospital rooms that they occupy. Will the HIPAA Privacy Rule allow the hospital to continue this practice?

### Answer:

The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure—for example, the disclosure to other patients in a waiting room of the identity of the person whose name is called. In this case, disclosure of patient names by posting on the wall is permitted by the Privacy Rule, if the use or disclosure is for treatment (for example, to ensure that patient care is provided to the correct individual) or health care operations purposes (for example, as a service for patients and their families). The disclosure of such information to other persons (such as other visitors) that will likely also occur due to the posting is an incidental disclosure.

Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate. [See our section on Incidental Uses and Disclosures](https://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html). In this case, it would appear that the disclosure of names is the minimum necessary for the purposes of the permitted uses or disclosures described above, and there do not appear to be additional safeguards that would be reasonable to take in these circumstances. However, each covered entity must evaluate what measures are reasonable and appropriate in its environment. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may tailor measures to their particular circumstances.

# May mental health practitioners or other specialists provide therapy to patients in a group setting where other patients and family members are present?

### Answer:

Yes. Disclosures of protected health information in a group therapy setting are treatment disclosures and, thus, may be made without an individual’s authorization. Furthermore, the HIPAA Privacy Rule generally permits a covered entity to disclose protected health information to a family member or other person involved in the individual’s care. Where the individual is present during the disclosure, the covered entity may disclose protected health information if it is reasonable to infer from the circumstances that the individual does not object to the disclosure. Absent countervailing circumstances, the individual’s agreement to participate in group therapy or family discussions is a good basis for inferring the individual’s agreement.

# Are covered entities required to document incidental disclosures permitted by the HIPAA Privacy Rule, in an accounting of disclosures provided to an individual?

### Answer:

No. The Privacy Rule includes a specific exception from the accounting standard for incidental disclosures permitted by the Rule. See [45 CFR 164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml)(a)(1).

Do the HIPAA Privacy Rule's provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?

Answer:

No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff. For example:

* A provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room.
* A health plan employee discussing a patient’s health care claim on the phone may be overheard by another employee who is not authorized to handle patient information.

If the provider and the health plan employee made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.

# Is a covered entity required to prevent any incidental use or disclosure of protected health information?

### Answer:

No. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures. See [45 CFR 164.530](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-530.xml)(c)(2).

# May a covered entity disclose protected health information in response to a court order?

### Answer:

Yes. A [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may disclose protected health information to comply with a court order, including an order of an administrative tribunal. Such disclosures must be limited to the protected health information expressly authorized by the order. See 45 CFR 164.512(e)(1)(i).

# May a covered entity use or disclose protected health information for litigation?

### Answer:

A [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may use or disclose protected health information as permitted or required by the Privacy Rule, see [45 CFR 164.502(a)](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html) (PDF); and, subject to certain conditions the Rule typically permits uses and disclosures for litigation, whether for judicial or administrative proceedings, under particular provisions for judicial and administrative proceedings set forth at [45 CFR 164.512(e)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml) (GPO), or as part of the covered entity’s health care operations, [45 CFR 164.506(a)](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html) (PDF). Depending on the context, a covered entity’s use or disclosure of protected health information in the course of litigation also may be permitted under a number of other provisions of the Rule, including uses or disclosures that are:

* required by law (as when the court has ordered certain disclosures),
* for a proceeding before a health oversight agency (as in a contested licensing revocation),
* for payment purposes (as in a collection action on an unpaid claim), or
* with the individual’s written authorization.

Where a covered entity is a party to a legal proceeding, such as a plaintiff or defendant, the covered entity may use or disclose protected health information for purposes of the litigation as part of its health care operations. The definition of “health care operations” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml) (GPO) includes a covered entity’s activities of conducting or arranging for legal services to the extent such activities are related to the covered entity’s covered functions (i.e., those functions that make the entity a health plan, health care provider, or health care clearinghouse), including legal services related to an entity’s treatment or payment functions. Thus, for example, a covered entity that is a defendant in a malpractice action or a plaintiff in a suit to obtain payment may use or disclose protected health information for such litigation as part of its health care operations. The covered entity, however, must make reasonable efforts to limit such uses and disclosures to the minimum necessary to accomplish the intended purpose. See [45 CFR 164.502(b)](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html) , 164.514(d).

Where the covered entity is not a party to the proceeding, the covered entity may disclose protected health information for the litigation in response to a court order, subpoena, discovery request, or other lawful process, provided the applicable requirements of [45 CFR 164.512(e)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml) (GPO) for disclosures for judicial and administrative proceedings are met.

# May a covered entity that is a plaintiff or defendant in a legal proceeding use or disclose protected health information for the litigation?

### Answer:

Yes. Where a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) is a party to a legal proceeding, such as a plaintiff or defendant, the covered entity may use or disclose protected health information for purposes of the litigation as part of its health care operations. The definition of “health care operations” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml) includes a covered entity’s activities of conducting or arranging for legal services to the extent such activities are related to the covered entity’s covered functions (i.e., those functions that make the entity a health plan, health care provider, or health care clearinghouse). Thus, for example, a covered entity that is a defendant in a malpractice action, or a plaintiff in a suit to obtain payment, may use or disclose protected health information for such litigation as part of its health care operations.

The covered entity, however, must make reasonable efforts to limit such uses and disclosures to the minimum necessary to accomplish the intended purpose. See [45 CFR 164.502(b)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml), [164.514(d)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml). In most cases, the covered entity will share protected health information for litigation purposes with its lawyer, who is either a workforce member or a business associate. In these cases, the Privacy Rule permits a covered entity to reasonably rely on the representations of a lawyer who is a business associate or workforce member that the information requested is the minimum necessary for the stated purpose. See 45 CFR 164.514(d)(3)(iii)(C). A covered entity’s minimum necessary policies and procedures may provide for such reasonable reliance on the lawyer’s requests for protected health information needed in the course of providing legal services to the covered entity.

In disclosing protected health information for litigation purposes, the lawyer who is a workforce member of the covered entity must make reasonable efforts to limit the protected health information disclosed to the minimum necessary for the purpose of the disclosure. Similarly, a lawyer who is a business associate must apply the minimum necessary standard to its disclosures, as the business associate contract may not authorize the business associate to further use or disclose protected health information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. Depending on the circumstances, this could involve de-identifying the information or stripping direct identifiers from the information to protect the privacy of individuals, and may in some cases limit disclosures more significantly than would be required to meet a “relevance” standard. Further, whether as workforce members or business associates, lawyers may consider availing themselves of the protections routinely afforded to similarly confidential information within the litigation forum, such as protective orders on the use of the information in public portions of the proceedings.

# What “satisfactory assurances” must a covered entity that is not a party to the litigation receive before it may respond to a subpoena without a court order?

### Answer:

Under [45 CFR 164.512(e)(1)(ii)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml) of the Privacy Rule, a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) that is not a party to the litigation may disclose protected health information in response to a subpoena, discovery request, or other lawful process if the covered entity receives certain satisfactory assurances from the party seeking the information. Specifically, the covered entity must receive a written statement and accompanying documentation that the requestor has made reasonable efforts either (1) to ensure that the individual(s) who are the subject of the information have been given sufficient notice of the request, or (2) to secure a qualified protective order. (Alternatively, the covered entity may make such disclosures if it itself makes reasonable efforts to notify the individual(s) or seek a qualified protective order.) If the conditions above have been met, a court order is not required to make the disclosure.

For notice to the individual(s), the written statement and accompanying documentation must demonstrate that the requestor has made a good faith attempt to provide written notice to the individual; and that the notice included sufficient information about the litigation to permit the individual to raise an objection with the court, the time for the individual to raise an objection has elapsed, and no objections were filed or all objections filed were resolved and the request is consistent with the resolution. Such statements and documentation may include, for example, a copy of the notice mailed to the individual that includes instructions for raising an objection with the court and the deadline for doing so, and a written statement or other documentation demonstrating that no objections were raised or all objections raised were resolved and the request is consistent with the resolution. To the extent that the subpoena or other request itself demonstrates the above elements, no additional documentation is required.

For a qualified protective order, the written statement and accompanying documentation must demonstrate that the parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or the party seeking the protected health information has requested a qualified protective order from the court or administrative tribunal. See the definition of “qualified protective order” at 45 CFR 164.512(e)(1)(v). Such statements and documentation may include, for example, a copy of the qualified protective order that the parties have agreed to and documentation or a statement that the order was presented to the court, or a copy of the motion to the court requesting a qualified protective order.

# For disclosures for judicial and administrative proceedings, can notice be provided to the individual's lawyer instead of the individual?

### Answer:

Yes. A [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) that is not a party to litigation must obtain or receive the satisfactory assurances required by [45 CFR 164.512(e)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml) before making a disclosure for a judicial or administrative proceeding. Where the satisfactory assurances are in the form of notice to the individual, a written statement and accompanying documentation of notice to the individual’s lawyer is considered to be notice to the individual and, thus, suffices, provided the documentation otherwise meets the requirements of 45 CFR 164.512(e)(1)(iii). Specifically, the written statement and accompanying documentation must demonstrate that the notice included sufficient information about the litigation to permit the individual to raise an objection to the court; and that the time for the individual to raise objections has elapsed, with no objections having been filed, or all filed objections having been resolved.

# For disclosures for judicial and administrative proceedings, when is a copy of the subpoena itself sufficient satisfactory assurance of notice to the individual?

### Answer:

A copy of the subpoena (or other request pursuant to lawful process) is sufficient when, on its face, it meets the requirements of [45 CFR 164.512(e)(1)(iii)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml), such as by demonstrating that the individual whose protected health information is requested is a party to the litigation, notice of the request has been provided to the individual or his or her attorney, and the time for the individual to raise objections has elapsed and no objections were filed or all objections filed have been resolved. When the above requirements are evident on the face of the subpoena (or other request), no additional documentation is required.

# When must a covered entity account for disclosures of protected health information made during the course of litigation?

### Answer:

Individuals have a right to receive, upon request, an accounting of disclosures of protected health information made by a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) (or its business associate), with certain exceptions. These exceptions, or instances where a covered entity is not required to account for disclosures, include disclosures for treatment, payment, or health care operations and disclosures authorized by the individual. See [45 CFR 164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml) (GPO). Disclosures that are subject to the accounting for disclosures requirement include disclosures made by a covered entity that is not a party to the litigation or proceeding and that are made:

1. as required by law (under §§ [164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(a) and (e)(1)(i));
2. for a proceeding before a health oversight agency (under § 164.512(d)); or
3. in response to a subpoena, discovery request, or other lawful process (under § 164.512(e)).

Conversely, covered entities need not account for disclosures of protected health information for litigation that are made with the individual’s authorization or, in cases where the covered entity is a party to the litigation, when such disclosures are part of the covered entity’s health care operations.

In many cases, covered entities share protected health information for litigation purposes with a lawyer who is a business associate of the covered entity. These disclosures by a covered entity to its lawyer-business associate are not themselves subject to the accounting. However, if (as described above) the lawyer makes disclosures that are subject to the accounting requirement, the business associate agreement required by the Privacy Rule must provide that the lawyer-business associate must make information about these disclosures available to the covered entity, so that the covered entity can fulfill its obligation to provide an accounting to the individual. Alternatively, the covered entity and the lawyer can agree through the business associate contract that the lawyer will provide the accounting to individuals who request one.

# May a covered entity that is not a party to a legal proceeding disclose protected health information in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order?

### Answer:

Yes, if certain conditions are met. A [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) that is not a party to litigation, such as where the covered entity is neither a plaintiff nor a defendant, may disclose protected health information in response to a subpoena, discovery request, or other lawful process, that is not accompanied by a court order, provided that the covered entity:

* Receives a written statement and accompanying documentation from the party seeking the information that reasonable efforts have been made either (1) to ensure that the individual(s) who are the subject of the information have been notified of the request, or (2) to secure a qualified protective order for the information; or
* Itself makes reasonable efforts either (1) to provide notice to the individual(s) that meets the same requirements as set forth below for sufficient notice by the party making the request, or (2) to seek a qualified protective order as defined below. See 45 CFR 164.512(e).

The covered entity must make reasonable efforts to limit the protected health information used or disclosed to the [minimum necessary](http://akatest3-ion-www.hhs.gov.edgekey-staging.net/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html) to respond to the request. See 45 CFR 164.502(b) and 164.514(d).

The requirement to provide sufficient notice to the individual(s) is met when a party provides a written statement and accompanying documentation that demonstrates:

* A good faith attempt was made to notify the individual (or if the individual’s location is unknown, to mail a notice to the individual’s last known address);
* The notice included sufficient detail to permit the individual to raise an objection with the court or administrative tribunal; and
* The time for the individual to raise objections under the rules of the court or tribunal has lapsed and no objections were filed or all objections filed by the individual have been resolved by the court and the disclosures being sought are consistent with the resolution.

A qualified protective order is an order of a court or administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and requires the return to the covered entity or destruction of the protected health information (including any copies) at the end of the litigation or proceeding. The party requesting the information must provide a written statement and accompanying documentation that demonstrates:
The parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or

* The party seeking the protected health information has requested a qualified protective order from the court or administrative tribunal.

# Must a covered entity provide an accounting for disclosures if the only information disclosed to a public health authority is in the form of a limited data set?

### Answer:

No, a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) is not required to provide an accounting for a disclosure where the only information disclosed is in the form of a limited data set, and the covered entity has a data use agreement with the public health authority receiving the information. (See [45 CFR 164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(e) for limited data set and data use agreement requirements.)

Moreover, a covered entity is not required to provide an accounting when it uses protected health information to create a limited data set. For example, when a covered entity’s workforce member – whether a paid employee or volunteer – reviews medical records to identify reportable cases and extracts facially unidentifiable information to be reported as part of a limited data set to the public health authority, the covered entity is using, rather than disclosing, protected health information. In that case, the covered entity does not have to provide an accounting for its uses of protected health information. Further, even though a disclosure occurs when the limited data set is received by the public health authority for its own public health purposes, the covered entity is not required to account for this disclosure. Limited data sets are excepted from the accounting requirement at [45 CFR 164.528(](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml)a)(1)(viii).

Does the HIPAA Privacy Rule expand the ability of providers, plans, marketers and others to use my protected health information to market goods and services to me? Does the Privacy Rule make it easier for health care businesses to engage in door-to-door sales and marketing efforts?

Answer:

No. The Privacy Rule’s limitations on the use or disclosure of protected health information for marketing purposes do not exist in most States today. For example, the Rule requires patients’ authorization for the following types of uses or disclosures of protected health information for marketing:

* Selling protected health information to third parties for their use and re-use. Thus, under the Rule, a hospital or other provider may not sell names of pregnant women to baby formula manufacturers or magazines without an authorization.
* Disclosing protected health information to outsiders for the outsiders’ independent marketing use. Under the Rule, doctors may not provide patient lists to pharmaceutical companies for those companies’ drug promotions without an authorization.

Without these Privacy Rule restrictions, these activities could occur with no authorization from the individual in most jurisdictions. In addition, if a State law provided additional limitations on disclosures of information for related activities, the Privacy Rule generally would not interfere with those laws.

Moreover, under the “business associate” provisions of the Privacy Rule, a covered entity may not give protected health information to a telemarketer, door-to-door salesperson, or other third party it has hired to make permitted communications (for example, about a covered entities’ own goods and services) unless that third party has agreed by contract to use the information only for communicating on behalf of the covered entity. Without the Privacy Rule, there may be no restrictions on how third parties re-use information they obtain from health plans and providers. See the fact sheet and frequently asked questions on this web site about the business associate standard for more information.

# Can contractors (business associates) use protected health information for its own marketing purposes?

### Answer

**No.** While covered entities may share protected health information with their contractors who meet the definition of “business associates” under the HIPAA Privacy Rule, that definition is limited to contractors that obtain protected health information to perform or assist in the performance of certain health care operations on behalf of covered entities. Thus, business associates, with limited exceptions, cannot use protected health information for their own purposes. Although, under the HIPAA statute, the Privacy Rule cannot govern contractors directly, the Rule does set clear parameters for how covered entities may contract with business associates. See [45 CFR 164.502(e)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml) and [164.504(e)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-504.xml), and the definition of “business associate” at [45 CFR 160.103](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-103.xml).

**Further, the Privacy Rule expressly prohibits health plans and covered health care providers from selling protected health information to third parties for the third party’s own marketing activities, without authorization.** So, for example, a pharmacist cannot, without patient authorization, sell a list of patients to a pharmaceutical company, for the pharmaceutical company to market its own products to the individuals on the list.

# Can telemarketers obtain my health information and use it to call me to sell good and services?

### Answer:

Under the HIPAA Privacy Rule, a covered entity can share protected health information with a telemarketer only if the covered entity has either obtained the individual’s prior written authorization to do so, or has entered into a business associate relationship with the telemarketer for the purpose of making a communication that is not marketing, such as to inform individuals about the covered entity’s own goods or services.

If the telemarketer is a business associate under the Privacy Rule, it must agree by contract to use the information only for communicating on behalf of the covered entity, and not to market its own goods or services (or those of another third party).

# How can I distinguish between activities for treatment or health care operations versus marketing activities?

### Answer:

The overlap among common usages of the terms “treatment,” “healthcare operations,” and “marketing” is unavoidable. For instance, in recommending treatments, providers and health plans sometimes advise patients to purchase goods and services. Similarly, when a health plan explains to its members the benefits it provides, it too is encouraging the use or purchase of goods and services.

The HIPAA Privacy Rule defines these terms specifically, so they can be distinguished. For example, the Privacy Rule excludes treatment communications and certain health care operations activities from the definition of “marketing.” If a communication falls under one of the definition’s exceptions, the marketing rules do not apply. In these cases, [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may engage in the activity without first obtaining an authorization. See the fact sheet on this web site about marketing, as well as the definition of “marketing” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml),for more information.

However, if a health care operation communication does not fall within one of these specific exceptions to the marketing definition, and the communication falls under the definition of “marketing,” the Privacy Rule’s provisions restricting the use or disclosure of protected health information for marketing purposes will apply. For these marketing communications, the individual’s authorization is required before a covered entity may use or disclose protected health information.

**Do disease management, health promotion, preventive care, and wellness programs fall under the HIPAA Privacy Rule's definition of "marketing"?**

**Answer:**

Generally, no. To the extent the disease management or wellness program is operated by the [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) directly or by a business associate, communications about such programs are not marketing because they are about the covered entity’s own health-related services. So, for example, a hospital’s Wellness Department could start a weight-loss program and send a flyer to all patients seen in the hospital over the past year who meet the definition of obese, even if those individuals were not specifically seen for obesity when they were in the hospital.

Moreover, a communication that merely promotes health in a general manner and does not promote a specific product or service from a particular provider does not meet the definition of “marketing.” Such communications may include population-based activities in the areas of health education or disease prevention. Examples of general health promotional material include:

* mailings reminding women to get an annual mammogram;
* mailings providing information about how to lower cholesterol, new developments in health care (e.g., new diagnostic tools),
* support groups,
* organ donation,
* cancer prevention, and
* health fairs.

# Is it marketing for a covered entity to describe products or services that are provided by the covered entity to its patients, or to describe products or services that are included in the health plan's plan of benefits of the health plan?

### Answer:

No. The HIPAA Privacy Rule excludes from the definition of “marketing” communications made to describe a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)’s health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication.

Thus, it would not be marketing for a physician who has developed a new anti-snore device to send a flyer describing it to all of her patients (whether or not each patient has actually sought treatment for snoring). Nor would it be marketing for an ophthalmologist or health plan to send existing patients or members discounts for eye-exams or eye-glasses available only to the patients and members. Similarly, it would not be marketing for an insurance plan to send its members a description of covered benefits, payment schedules, and claims procedures.

# Is it marketing for a covered entity to describe the entities participating in a health care provider network or a health plan network?

### Answer:

No. The HIPAA Privacy Rule excludes from the definition of “marketing,” communications by a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to describe the entities participating in a health care provider network or a health plan network. Thus, it would not be marketing for a health plan or insurer to mail its members or enrollees a list of health care providers in the health plan network or for an independent physicians association to send its patients a preferred provider list.

# Is it marketing for an insurance plan or health plan to send enrollees notices about changes, replacements, or improvements to existing plans?

### Answer

No. The HIPAA Privacy Rule excludes from the definition of “marketing,” communications about replacements of, or enhancements to, a health plan. Therefore, notices about changes in deductibles, co-pays and types of coverage, such as prescription drugs, are not marketing. Likewise, a notice to a family warning that a student reaching the age of majority on a parental policy will lose coverage, then offering continuation coverage, would not be considered marketing. Nor are special health care policies such as guaranteed issue products and conversion policies considered marketing. Similarly, notices from a health plan about its long term care benefits would not be considered marketing.

It would be considered marketing, however, for a health plan to send to its members promotional material about insurance products that are considered to be “excepted benefits” (described in section 2791(c)(1) of the Public Health Service Act), such as accident only policies. It would likewise be marketing for health plans to describe other lines of insurance, such as life insurance policies. Generally, such communications require authorizations.

# Can health plans communicate about health-related products or services to enrollees that add value to, but are not part of, a plan of benefits?

### Answer:

Yes. The provision of value-added items or services (VAIS) is a common practice, particularly for managed care organizations. Under the HIPAA Privacy Rule, communications may qualify under the marketing exception for a communication about a health plan’s plan of benefits, even if the VAIS are not considered plan benefits for the Adjusted Community Rate purposes. To qualify for this exclusion, however, the VAIS must meet two conditions. First, they must be health-related. Therefore, discounts offered by Medicare + Choice or other managed care organizations for eyeglasses may be considered part of the plan’s benefits, whereas discounts to attend movie theaters will not. Second, such items and services must demonstrably “add value” to the plan’s membership and not merely be a pass-through of a discount or item available to the public at large.

So, a Medicare + Choice or other managed care organization could offer its members a special discount opportunity for eyeglasses and contact lenses without obtaining authorizations if the discount were only available through membership in the managed care organization. However, such communications would need an authorization if the members would be able to obtain such discounts directly from the eyeglass store. Similarly, a Medicare + Choice or other managed care organization could offer its members a special discount opportunity for a prescription drug card benefit or for a health/fitness club membership, which is not available to consumers on the open market. On the other hand, a Medicare+Choice or other managed care organization would need an authorization to notify its members of a discount to a movie theater available only to its members.

# Can a doctor or pharmacy be paid to make a prescription refill reminder without a prior authorization under the HIPAA Privacy Rule?

### Answer:

Yes. It is not marketing for a doctor to make a prescription refill reminder even if a third party pays for the communication. The prescription refill reminder is considered treatment. The communication is therefore excluded from the definition of marketing and does not require a prior authorization. Similarly, it is not marketing when a doctor or pharmacy is paid by a pharmaceutical company to recommend an alternative medication to patients. Communications about alternative treatments are excluded from the definition of marketing and do not require a prior authorization. The simple receipt of remuneration does not transform a treatment communication into a commercial promotion of a product or service.

Furthermore, [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may use a legitimate business associate to assist them in making such permissible communications. For instance, if a pharmacist that has been paid by a third party contracts with a mail house to send out prescription refill reminders to the pharmacist’s patients, neither the mail house nor the pharmacist needs a prior authorization. However, a covered entity would require an authorization if it sold protected health information to a third party for the third party’s marketing purposes.

# What are examples of "alternative treatments" that are excepted from the HIPAA Privacy Rule's definition of "marketing"?

### Answer:

Alternative treatments are treatments that are within the range of treatment options available to an individual. For example, it would be an alternative treatment communication if a doctor, in response to an inquiry from a patient with skin rash about the range of treatment options, mails the patient a letter recommending that the patient purchase various ointments and medications described in brochures enclosed with the letter.

Alternative treatment could also include alternative medicine. Thus, alternative treatments would include communications by a nurse midwife who recommends or sells vitamins and herbal preparations, dietary and exercise programs, massage services, music or other alternative types of therapy to her pregnant patients.

# Are prior authorizations required when a doctor or health plan distributes promotional gifts of nominal value?

### Answer:

No. In a specific exception, the HIPAA Privacy Rule allows [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to distribute items commonly known as promotional gifts of nominal value without prior authorization, even if such items are distributed with the intent of encouraging the receiver to buy the products or services.

This authorization exception generally applies to items and services of a third party, whether or not they are health-related, or items and services of the covered entity that are not health-related. A covered doctor, for instance, may send patients items such as pens, note-pads, and cups embossed with a health plan’s logo without prior authorization. Similarly, dentists may give patients free toothbrushes, floss and toothpaste.

# Are health care providers required to seek a prior authorization before discussing a product or service with a patient, or giving a product or service to a patient, in a face-to-face encounter?

### Answer:

No. In face-to-face encounters, the HIPAA Privacy Rule allows [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to give or discuss products or services, even when not health-related, to patients without a prior authorization. This exception prevents unnecessary intrusion into the doctor-patient relationship.

Physicians may give out free pharmaceutical samples, regardless of their value. Similarly, hospitals may give infant supplies to new mothers. Moreover, the face-to-face exception would allow providers to leave general circulation materials in their offices for patients to pick up during office visits.

# Must insurance agents that are business associates of a health plan seek a prior authorization before talking to a customer in a face-to-face encounter about the insurance company's other lines of business?

### Answer:

No. In the specific case of face-to-face encounters, the HIPAA Privacy Rule allows health plans and their business associates to market both health and non-health insurance products to individuals.

# What effect do the “marketing” provisions of the HIPAA Privacy Rule have on Federal or State fraud and abuse statutes?

### Answer:

The Privacy Rule makes it clear that nothing in the marketing provisions of the Privacy Rule are to be construed as amending, modifying, or changing any rule or requirement related to any other Federal or State statutes or regulations, including specifically anti-kickback, fraud and abuse, or self-referral statutes or regulations, or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations. Examples of such laws include:

* the anti-kickback statute (section 1128B(b) of the Social Security Act),
* safe harbor regulations (42 CFR Parts 411 and 424), and
* HIPAA statute on self-referral (section 1128C of the Social Security Act).

The definition of “marketing” is applicable solely to the Privacy Rule and the permissions granted by the Rule are only for a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)’s use or disclosure of protected health information. In particular, although the Privacy Rule defines the term “marketing” to exclude communications to an individual to recommend, purchase, or use a product or service as part of the treatment of the individual or for case management or care coordination of that individual, such communication by a health care professional may violate the anti-kickback statute.

Similar examples of pharmacist communications with patients relating to the marketing of products on behalf of pharmaceutical companies were identified by the Office of the Inspector General (OIG) as problematic in a 1994 Special Fraud Alert (December 19, 1994, 59 FR 65372). Other violations have involved home health nurses and physical therapists acting as marketers for durable medical equipment companies. Although a particular communication under the Privacy Rule may not require patient authorization because it is not “marketing,” or may require patient authorization because it is “marketing” as the Rule defines it, the arrangement may nevertheless violate other statutes and regulations administered by the Department of Health and Human Services, Department of Justice, or other Federal or State agencies.

# May covered entities use information regarding specific clinical conditions of individuals in order to communicate about products or services for such conditions without a prior authorization?

### Answer:

Yes, if the communication is for the individual’s treatment or for case management, care coordination, or the recommendation of alternative therapies. The HIPAA Privacy Rule permits the use of clinical information to the extent it is reasonably necessary for these communications. Similarly, population-based activities in the areas of health education or disease prevention are not considered marketing when they promote health in a general manner. Again clinical information may be used for such communications, such as in targeting a public education campaign.

# Are communications concerning information to beneficiaries about government programs or government-sponsored programs "marketing" under the HIPAA Privacy Rule?

### Answer:

No. Communications about government and government-sponsored programs do not fall within the definition of “marketing.” There is no commercial component to communications about benefits available through public programs. Therefore, a [covered entit](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)y is permitted to use and disclose protected health information to communicate about eligibility for such programs as Medicare, Medicaid, or the State Children’s Health Insurance Program (SCHIP).

# What types of communications fall within the “refill reminder” exception to marketing?

### Answer:

The refill reminder exception to the definition of “marketing” encompasses refill reminders and other communications about a drug or biologic that is currently being prescribed for the individual. See paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501. In addition to refill reminders about currently prescribed drugs, the exception encompasses communications about generic equivalents of a drug being prescribed, adherence communications encouraging individuals to take prescribed medicines as directed, and communications about prescriptions that have lapsed within the last 90 calendar days. Also, where an individual is prescribed a self-administered drug, communications regarding all aspects of a drug delivery system fall within the refill reminder exception. Thus, these types of communications are permitted without an individual’s authorization, provided any financial remuneration received from the pharmaceutical manufacturer in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.

# Do communications about recently-lapsed prescriptions for a medicine fall within the “refill reminder” exception to marketing?

### Answer:

Yes, so long the prescription lapsed within the last 90 calendar days and any financial remuneration received in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.  Communications encouraging individuals to renew recently lapsed prescriptions are consistent with the purpose of refill reminder and medication adherence communications, which is to encourage individuals to continue to take their medication as directed.  However, once a prescription has lapsed for more than 90 calendar days, it is no longer reasonable to treat such communications as refill reminders or medication adherence communications for a currently prescribed drug or biologic.

# Do communications about drug delivery systems fall within the “refill reminder” exception to marketing?

### Answer:

Yes.  Where an individual is prescribed a self-administered drug or biologic, such as insulin, communications regarding all aspects of a drug delivery system, such as an insulin pump, fall within the refill reminder exception at paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501, provided any financial remuneration received in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.

# Do communications about specific adjunctive drugs related to the currently prescribed drug fall within the “refill reminder” exception to marketing?

### Answer:

No, only communications about drugs or biologics currently prescribed to the individual fall within the refill reminder exception at paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501. An adjunctive drug that may be used in conjunction with a currently prescribed drug to help treat a patient’s underlying condition or address one or more side effects of a currently prescribed drug does not fall within this category. However, covered entities may communicate in a general manner to individuals regarding the availability of adjunctive drugs related to the drug that is currently being prescribed to the individual without triggering the marketing requirements. For example, a pharmacy could send a communication to an individual alerting the individual to possible side effects from her currently prescribed medication, and suggesting the individual go ask her doctor about a medication to treat the side effects if she experiences them, without naming a particular medication. Alternatively, communications about adjunctive drugs may fall within the treatment exception to marketing at paragraph (2)(ii)(A) of the definition, provided the covered entity does not receive financial remuneration in exchange for making the communication. In addition, such communications may be made in a face-to-face encounter with the individual, without authorization, even if financial remuneration is received in exchange for making the communication.

# Do communications about new formulations of a currently prescribed medicine fall within the “refill reminder” exception to marketing?

### Answer:

No, only communications about drugs or biologics currently prescribed to the individual fall within the refill reminder exception at paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501. However, covered entities may communicate in a general manner to individuals regarding the availability of a drug with, for example, a different dosing schedule or form, without triggering the marketing requirements. For example, a pharmacy could send an adherence communication to an individual that also informs the individual about the availability of a product with a more convenient dosing schedule or in a liquid instead of pill format, without naming the particular medication. Alternatively, communications about specific new formulations of a drug may fall within the treatment exception to marketing at paragraph (2)(ii)(A) of the definition, provided the covered entity does not receive financial remuneration in exchange for making the communication. In addition, such communications may be made in a face-to-face encounter with the individual, without authorization, even if financial remuneration is received in exchange for making the communication.

# Do communications encouraging individuals to switch from a prescribed medicine to an alternative therapy fall within the “refill reminder” exception to marketing?

### Answer

No, only communications about drugs or biologics currently prescribed to the individual fall within the refill reminder exception at paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501. Making a communication to an individual encouraging the individual to switch from a prescribed medicine to an alternative therapy would only be appropriate where such communication falls within the treatment exception to marketing at paragraph (2)(ii)(A) of the definition and the covered entity does not receive financial remuneration in exchange for making the communication; where the communication is made in a face-to-face encounter with the individual; or where the individual has authorized the use or disclosure of her protected health information to make such communications.

What is permitted remuneration for purposes of the “refill reminder” exception to marketing?

Answer:

The Privacy Rule excepts from the definition of “marketing” refill reminders and other communications about a drug or biologic that is currently being prescribed for the individual, provided that financial remuneration received by the covered entity in exchange for making the communication, if any, is reasonably related to the covered entity’s cost of making the communication.  See paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501.  Financial remuneration means payment to a covered entity (or business associate, if applicable) from or on behalf of a third party whose product or service is being described.  Thus, for these purposes, permitted remuneration in exchange for making a “refill reminder” communication is:

* Non-financial or in-kind remuneration, such as supplies, computers, or other materials.
* Payment from a party other than the third party (or other than on behalf of the third party) whose product or service is being described in the communication, such as payment from a health plan.
* Payments to a covered entity by a pharmaceutical manufacturer or other third party whose product is being described in the communication that cover only the reasonable direct and indirect costs related to the refill reminder or medication adherence program, or other excepted communications, including labor, materials, and supplies, as well as capital and overhead costs.

Where a covered entity enlists the services of a business associate to assist in carrying out a refill reminder or medication adherence program, or to make other excepted communications, the business associate may be paid by the third party (either directly or through the covered entity) only up to the fair market value of its services.

# May a covered entity pay a business associate to assist in making a refill reminder or other communication that falls within the “refill reminder” exception to marketing?

### Answer:

Yes.  The Privacy Rule permits a covered entity to engage and pay a business associate to assist in making otherwise permitted communications to individuals and does not prescribe what the covered entity itself may pay the business associate for such services.  However, where financial remuneration is received from the pharmaceutical manufacturer or other third party whose product is being described to make such communications, there are limits on what the business associate may be paid from that financial remuneration.  In particular, a business associate only may receive, whether directly from the third party or through the covered entity from the financial remuneration the covered entity receives from the third party, payments not to exceed the fair market value of its services.

# May a business associate be paid by a pharmaceutical manufacturer to assist a covered entity in making a refill reminder or other communication describing the manufacturer’s product that falls within the “refill reminder” exception to marketing?

### Answer

Yes, provided any payments to the business associate do not exceed the fair market value of its services.  See paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501.  The payments may be made by a pharmaceutical manufacturer through a covered entity to the business associate, or directly to the business associate, that is acting on behalf of the covered entity to assist in making the refill reminder or other communication describing the manufacturer’s product.

# May a covered entity contract with a business associate to assist in administering a refill reminder or medication adherence program paid for by a pharmaceutical manufacturer?

### Answer:

Yes.  However, in order for the refill reminders or other program communications to fall within the “refill reminder” exception to marketing, any financial remuneration received by the business associate from the pharmaceutical manufacturer (either directly or through the covered entity) must not exceed the fair market value of the business associate’s services.  See paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501.  Such limitations do not apply to what the covered entity itself may pay the business associate for such services when no financial remuneration is received from the pharmaceutical manufacturer or other third party whose product or service is being described.

# We operate specialty pharmacy programs that make pharmaceutical manufacturer-funded communications to patients concerning their prescribed drugs for chronic and complex diseases that require complicated therapies. Rather than ensure such communications meet the conditions of the “refill reminder” exception at paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501 of the Privacy Rule, we have decided to obtain authorizations going forward for such communications from new patients as they enroll in the programs. For existing patients, must we either obtain authorizations by the September 23, 2013, compliance date of the new provisions or terminate these sponsored communications with these patients?

### Answer:

No.  With respect to obtaining authorizations from patients already enrolled in these programs, OCR will not determine that a covered entity is in violation of the marketing provisions if it has not obtained authorizations from all existing patients to whom it is making such communications by the September 23, 2013, compliance date, provided the patients from whom authorizations have not been obtained have not opted out or declined to receive such communications and the patients’ authorizations are obtained at the next time their prescriptions are renewed, but no later than September 23, 2014.

# If a covered entity is going to obtain authorizations from patients to make pharmaceutical manufacturer-funded communications to the patients about currently prescribed drugs or biologics, is the covered entity required to obtain a new authorization each time a prescription is renewed?

### Answer:

No.  A HIPAA authorization remains valid until it expires or is revoked by the individual.  While a HIPAA authorization must contain an expiration date or event that relates to the individual or the purpose of the use or disclosure, the Privacy Rule does not otherwise prescribe the expiration date or event that must apply to the authorization, which may vary based on the circumstances.  For example, in the case of communications to individuals concerning currently prescribed drugs, a HIPAA authorization could expire at the time, or within a specified period of time after, a prescription expires or is no longer valid; or at the time a patient opts out of receiving such communications from the covered entity or opts out of participating in the prescription drug adherence or education program.  Further, the scope of the authorization need not be limited to communications related to a single drug or biologic or the drugs or biologics of only one pharmaceutical manufacturer.  The authorization must adequately describe the intended purposes of the requested uses and disclosures and otherwise contain the elements and statements of a valid authorization under 45 CFR 164.508.  For these purposes, this includes stating in the authorization that the covered entity is receiving financial remuneration from one or more pharmaceutical manufacturers to make the communications, and that the individual may revoke the authorization in writing at any time he or she wishes to stop receiving the communications.

# Are pharmaceutical manufacturer-funded communications to patients concerning a prescribed drug considered marketing under the Privacy Rule if they are required by a Risk Evaluation and Mitigation Strategy (REMS)?

### Answer:

No. If the Food and Drug Administration (FDA) determines that a particular drug can only be approved with additional measures, beyond labeling, to mitigate a serious risk posed by the drug, and one or more of those measures take the form of patient communications about the drug, then such communications are not marketing, even if the communication is funded by the drug manufacturer. Government-mandated communications to individuals are not considered marketing under the Privacy Rule, even if such communications are paid for by a third party whose product or service is being described. As with communications to individuals concerning government and government-sponsored programs, government-mandated communications to individuals are not commercial in nature. Thus, a covered entity may use or disclose an individual’s protected health information without the individual’s authorization to send the individual educational or other information concerning a prescribed drug that is required by a REMS, even if the communication is funded by the drug manufacturer.

# Must a pharmacy obtain an individual’s written authorization prior to discussing with the individual an alternative medication to the one prescribed to the individual in a face-to-face encounter?

### Answer:

No.  Face-to-face communications with an individual about specific products or services do not require individual authorization, even if such communications are subsidized by the third party whose product or service is being described.  See 45 CFR 164.508(a)(3)(i)(A).  Thus, a pharmacy or other covered entity may discuss with, or hand printed information to, an individual about particular medicines in a face-to-face encounter, without triggering the individual authorization requirements of the HIPAA Privacy Rule.  However, face-to-face communications do not include communications over the telephone or by e-mail or mail.

# Can the personal representative of an adult or emancipated minor obtain access to the individual's medical record?

### Answer:

The HIPAA Privacy Rule treats an adult or emancipated minor’s personal representative as the individual for purposes of the Rule regarding the health care matters that relate to the representation, including the right of access under [45 CFR 164.524](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-524.xml). The scope of access will depend on the authority granted to the personal representative by other law. If the personal representative is authorized to make health care decisions, generally, then the personal representative may have access to the individual’s protected health information regarding health care in general. On the other hand, if the authority is limited, the personal representative may have access only to protected health information that may be relevant to making decisions within the personal representative’s authority. For example, if a personal representative’s authority is limited to authorizing artificial life support, then the personal representative’s access to protected health information is limited to that information which may be relevant to decisions about artificial life support.

There is an exception to the general rule that a covered entity must treat an adult or emancipated minor’s personal representative as the individual. Specifically, the Privacy Rule does not require a covered entity to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. This exception applies to adults and both emancipated and unemancipated minors who may be subject to abuse or neglect by their personal representatives.

Does the HIPAA Privacy Rule allow parents the right to see their children’s medical records?

Answer:

Yes, the Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child’s personal representative when such access is not inconsistent with State or other law.

There are three situations when the parent would not be the minor’s personal representative under the Privacy Rule. These exceptions are:

1. When the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law;
2. When the minor obtains care at the direction of a court or a person appointed by the court; and
3. When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

However, even in these exceptional situations, the parent may have access to the medical records of the minor related to this treatment when State or other applicable law requires or permits such parental access. Parental access would be denied when State or other law prohibits such access. If State or other applicable law is silent on a parent’s right of access in these cases, the licensed health care provider may exercise his or her professional judgment to the extent allowed by law to grant or deny parental access to the minor’s medical information.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child’s personal representative could endanger the child.

# At what age of a child is the parent no longer the personal representative of the child for HIPAA purposes?

HIPAA defers to state law to determine the age of majority and the rights of parents to act for a child in making health care decisions, and thus, the ability of the parent to act as the personal representative of the child for HIPAA purposes. See 45 CFR 164.502(g).

# Does having a health care power of attorney (POA) allow access to the patient’s medical and mental health records under HIPAA?

### Answer:

Generally, yes. If a health care power of attorney is currently in effect, the named person would be the patient’s personal representative (The period of effectiveness may depend on the type of power of attorney: Some health care power of attorney documents are effective immediately, while others are only triggered if and when the patient lacks the capacity to make health care decisions and then cease to be effective if and when the patient regains such capacity).

“Personal representatives,” as defined by HIPAA, are those persons who have authority, under applicable law, to make health care decisions for a patient. HIPAA provides a personal representative of a patient with the same rights to access health information as the patient, including the right to request a complete medical record containing mental health information. The patient’s right of access has some exceptions, which would also apply to a personal representative. For example, with respect to mental health information, a psychotherapist’s separate notes of counseling sessions, kept separately from the patient chart, are not included in the HIPAA right of access.

Additionally, a provider may decide not to treat someone as the patient’s personal representative if the provider believes that the patient has been or may be subject to violence, abuse, or neglect by the designated person or the patient may be endangered by treating such person as the personal representative, and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the person as the personal representative. See 45 CFR 164.502(g)(5).

# When an individual reaches the age of majority or becomes emancipated, who controls the protected health information concerning health care services rendered while the individual was an unemancipated minor?

### Answer:

The individual who is the subject of the protected health information can exercise all rights granted by the HIPAA Privacy Rule with respect to all protected health information about him or her, including information obtained while the individual was an unemancipated minor consistent with State or other law. Generally, the parent would no longer be the personal representative of his or her child once the child reaches the age of majority or becomes emancipated, and therefore, would no longer control the health information about his or her child. Of course, any individual can have a personal representative – which may include a parent – who can exercise rights on his or her behalf.

# May a psychologist continue his practice to notify a parent before treating his or her minor child, even though the minor child is able to consent to such health care under state law?

### Answer

The HIPAA Privacy Rule would defer to State or other applicable law that addresses the disclosure of health information to a parent about a minor child. If the minor child is permitted, under State law, to consent to such health care without the consent of her parent and does consent to such care, the provider may notify the parent when the State law explicitly requires or permits the health provider to do so. If State law permits the minor child to consent to such health care without parental consent, but is silent on parental notification, the provider would need the child’s permission to notify a parent.

# Can a minor child’s doctor talk to the child’s parent about the patient’s mental health status and needs?

With respect to general treatment situations, a parent, guardian, or other person acting in loco parentis usually is the personal representative of the minor child, and a health care provider is permitted to share patient information with a patient’s personal representative under the Privacy Rule. However, section 164.502(g) of the Privacy Rule contains several important exceptions to this general rule. A parent is not treated as a minor child’s personal representative when: (1) State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, the minor consents to the health care service, and the minor child has not requested the parent be treated as a personal representative; (2) someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent; or (3) a parent agrees to a confidential relationship between the minor and a health care provider with respect to the health care service.2 For example, if State law provides an adolescent the right to obtain mental health treatment without parental consent, and the adolescent consents to such treatment, the parent would not be the personal representative of the adolescent with respect to that mental health treatment information.

Regardless, however, of whether the parent is otherwise considered a personal representative, the Privacy Rule defers to State or other applicable laws that expressly address the ability of the parent to obtain health information about the minor child. In doing so, the Privacy Rule permits a covered entity to disclose to a parent, or provide the parent with access to, a minor child’s protected health information when and to the extent it is permitted or required by State or other laws (including relevant case law). Likewise, the Privacy Rule prohibits a covered entity from disclosing a minor child’s protected health information to a parent when and to the extent it is prohibited under State or other laws (including relevant case law). See 45 CFR 164.502(g)(3)(ii).

In cases in which State or other applicable law is silent concerning disclosing a minor’s protected health information to a parent, and the parent is not the personal representative of the minor child based on one of the exceptional circumstances described above, a covered entity has discretion to provide or deny a parent access to the minor’s health information, if doing so is consistent with State or other applicable law, and the decision is made by a licensed health care professional in the exercise of professional judgment. For more information about personal representatives under the Privacy Rule, see OCR’s guidance for [consumers](https://www.hhs.gov/hipaa/for-individuals/personal-representatives/index.html) and [providers](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html).

In situations where a minor patient is being treated for a mental health disorder and a substance abuse disorder, additional laws may be applicable. The Federal confidentiality statute and regulations that apply to federally-funded drug and alcohol abuse treatment programs contain provisions that are more stringent than HIPAA. See 42 USC § 290dd–2; 42 CFR 2.11, et. seq.

Note: A parent also may not be a personal representative if there are safety concerns. A provider may decide not to treat the parent as the minor’s personal representative if the provider believes that the minor has been or may be subject to violence, abuse, or neglect by the parent or the minor may be endangered by treating the parent as the personal representative; and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the parent as the personal representative. See 45 CFR 164.502(g)(5).

# Does a parent have a right to receive a copy of psychotherapy notes about a child’s mental health treatment?

No. The Privacy Rule distinguishes between mental health information in a mental health professional’s private notes and that contained in the medical record. It does not provide a right of access to psychotherapy notes, which the Privacy Rule defines as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient’s medical record. See 45 CFR 164.501. Psychotherapy notes are primarily for personal use by the treating professional and generally are not disclosed for other purposes. Thus, the Privacy Rule includes an exception to an individual’s (or personal representative’s) right of access for psychotherapy notes. See 45 CFR 164.524(a)(1)(i).

However, parents generally are the personal representatives of their minor child and, as such, are able to receive a copy of their child’s mental health information contained in the medical record, including information about diagnosis, symptoms, treatment plans, etc. Further, although the Privacy Rule does not provide a right for a patient or personal representative to access psychotherapy notes regarding the patient, HIPAA generally gives providers discretion to disclose the individual’s own protected health information (including psychotherapy notes) directly to the individual or the individual’s personal representative. As any such disclosure is purely permissive under the Privacy Rule, mental health providers should consult applicable State law for any prohibitions or conditions before making such disclosures.

# Does HIPAA allow a health care provider to communicate with a patient’s family, friends, or other persons who are involved in the patient’s care?

Yes. In recognition of the integral role that family and friends play in a patient’s health care, the HIPAA Privacy Rule allows these routine – and often critical – communications between health care providers and these persons. Where a patient is present and has the capacity to make health care decisions, health care providers may communicate with a patient’s family members, friends, or other persons the patient has involved in his or her health care or payment for care, so long as the patient does not object. See 45 CFR 164.510(b). The provider may ask the patient’s permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment, that the patient does not object. A common example of the latter would be situations in which a family member or friend is invited by the patient and present in the treatment room with the patient and the provider when a disclosure is made.

Where a patient is not present or is incapacitated, a health care provider may share the patient’s information with family, friends, or others involved in the patient’s care or payment for care, as long as the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient. Note that, when someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care.

In all cases, disclosures to family members, friends, or other persons involved in the patient’s care or payment for care are to be limited to only the protected health information directly relevant to the person’s involvement in the patient’s care or payment for care.

OCR’s website contains additional information about disclosures to family members and friends in fact sheets developed for [consumers](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/sharing-family-friends.pdf) and [providers](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf).

Is a health care provider permitted to discuss an adult patient’s mental health information with the patient’s parents or other family members?

In situations where the patient is given the opportunity and does not object, HIPAA allows the provider to share or discuss the patient’s mental health information with family members or other persons involved in the patient’s care or payment for care. For example, if the patient does not object:

* A psychiatrist may discuss the drugs a patient needs to take with the patient’s sister who is present with the patient at a mental health care appointment.
* A therapist may give information to a patient’s spouse about warning signs that may signal a developing emergency.

But:

* A nurse may not discuss a patient’s mental health condition with the patient’s brother after the patient has stated she does not want her family to know about her condition.

In all cases, the health care provider may share or discuss only the information that the person involved needs to know about the patient’s care or payment for care. See 45 CFR 164.510(b). Finally, it is important to remember that other applicable law (e.g., State confidentiality statutes) or professional ethics may impose stricter limitations on sharing personal health information, particularly where the information relates to a patient’s mental health.

# When does mental illness or another mental condition constitute incapacity under the Privacy Rule? For example, what if a patient who is experiencing temporary psychosis or is intoxicated does not have the capacity to agree or object to a health care provider sharing information with a family member, but the provider believes the disclosure is in the patient’s best interests?

Section 164.510(b)(3) of the HIPAA Privacy Rule permits a health care provider, when a patient is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing a patient’s information to the patient’s family, friends, or other persons involved in the patient’s care or payment for care, is in the best interests of the patient. Where a provider determines that such a disclosure is in the patient’s best interests, the provider would be permitted to disclose only the PHI that is directly relevant to the person’s involvement in the patient’s care or payment for care.

This permission clearly applies where a patient is unconscious. However, there may be additional situations in which a health care provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to the sharing of personal health information at a particular time and that sharing the information is in the best interests of the patient at that time. These may include circumstances in which a patient is suffering from temporary psychosis or is under the influence of drugs or alcohol. If, for example, the provider believes the patient cannot meaningfully agree or object to the sharing of the patient’s information with family, friends, or other persons involved in their care due to her current mental state, the provider is allowed to discuss the patient’s condition or treatment with a family member, if the provider believes it would be in the patient’s best interests. In making this determination about the patient’s best interests, the provider should take into account the patient’s prior expressed preferences regarding disclosures of their information, if any, as well as the circumstances of the current situation. Once the patient regains the capacity to make these choices for herself, the provider should offer the patient the opportunity to agree or object to any future sharing of her information.

\*Note: The Privacy Rule permits, but does not require, providers to disclose information in these situations. Providers who are subject to more stringent privacy standards under other laws, such as certain state confidentiality laws or 42 CFR Part 2, would need to consider whether there is a similar disclosure permission under those laws that would apply in the circumstances.

# If a health care provider knows that a patient with a serious mental illness has stopped taking a prescribed medication, can the provider tell the patient’s family members?

So long as the patient does not object, HIPAA allows the provider to share or discuss a patient’s mental health information with the patient’s family members. See 45 CFR 164.510(b). If the provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to sharing the information at that time, and that sharing the information would be in the patient’s best interests, the provider may tell the patient’s family member. In either case, the health care provider may share or discuss only the information that the family member involved needs to know about the patient’s care or payment for care.

Otherwise, if the patient has capacity and objects to the provider sharing information with the patient’s family member, the provider may only share the information if doing so is consistent with applicable law and standards of ethical conduct, and the provider has a good faith belief that the patient poses a threat to the health or safety of the patient or others, and the family member is reasonably able to prevent or lessen that threat. See 45 CFR 164.512(j). For example, if a doctor knows from experience that, when a patient’s medication is not at a therapeutic level, the patient is at high risk of committing suicide, the doctor may believe in good faith that disclosure is necessary to prevent or lessen the threat of harm to the health or safety of the patient who has stopped taking the prescribed medication, and may share information with the patient’s family or other caregivers who can avert the threat. However, absent a good faith belief that the disclosure is necessary to prevent a serious and imminent threat to the health or safety of the patient or others, the doctor must respect the wishes of the patient with respect to the disclosure.

# When does HIPAA allow a doctor to notify an individual’s family, friends, or caregivers that a patient has overdosed?

### Answer:

As explained more thoroughly below, when a patient has overdosed, a health care professional, such as a doctor, generally may notify the patient’s family, friends, or caregivers involved in the patient’s health care or payment for care if:

(1) the patient has the capacity to make health care decisions at the time of the disclosure, is given the opportunity to object, and does not object;

(2) the family, friends, or caregivers have been involved in the patient’s health care or payment for care and there has been no objection from the patient;

(3) the patient had the capacity to make health care decisions at the time the information is shared and the doctor can reasonably infer, based on the exercise of professional judgment, that the patient would not object;

(4) the patient is incapacitated and the health care professional determines, based on the exercise of professional judgment, that notification and disclosure of PHI is in the patient’s best interests;

(5) the patient is unavailable due to some emergency and the health care professional determines, based on the exercise of professional judgment, that notification and disclosure of PHI is in the patient’s best interests; or

(6) the notification is necessary to prevent a serious and imminent threat to the health or safety of the patient or others.

If the patient who has overdosed is incapacitated and unable to agree or object, a doctor may notify a family member, personal representative, or another person responsible for the individual’s care of the patient’s location, general condition, or death. See 45 CFR 164.510(b)(1)(ii). Similarly, HIPAA allows a doctor to share additional information with a patient’s family member, friend, or caregiver as long as the information shared is directly related to the person’s involvement in the patient's health care or payment for care. 45 CFR 164.510(b)(1)(i). Decision-making incapacity may be temporary or long-term. If a patient who has overdosed regains decision-making capacity, health providers must offer the patient the opportunity to agree or object to sharing their health information with involved family, friends, or caregivers before making any further disclosures. If a patient becomes unavailable due to some emergency, a health care professional may determine, based on the exercise of professional judgment, that notification and disclosure of PHI to someone previously involved in their care is in the patient’s best interests. For example, if a patient who is addicted to opioids misses important medical appointments without any explanation, a primary health care provider at a general practice may believe that there is an emergency related to the opioid addiction and under the circumstances, may use professional judgment to determine that it is in the patient’s best interests to reach out to emergency contacts, such as parents or family, and inform them of the situation. See 45 CFR 164.510(b)(3).

If the patient is deceased, a doctor may disclose information related to the family member’s, friend’s, or caregiver’s involvement with the patient’s care, unless doing so is inconsistent with any prior expressed preference of the patient that is known to the doctor. If the person who will receive notification is the patient's personal representative, that person has a right to request and obtain any information about the patient that the patient could obtain, including a complete medical record, under the HIPAA right of access. See 45 CFR 164.524.

When a patient poses a serious and imminent threat to his own or someone else’s health or safety, HIPAA permits a health care professional to share the necessary information about the patient with anyone who is in a position to prevent or lessen the threatened harm--including family, friends, and caregivers--without the patient’s permission. See 45 CFR 164.512(j). HIPAA expressly defers to the professional judgment of health care professionals when they make determinations about the nature and severity of the threat to health or safety. See 45 CFR 164.512(j)(4). Specifically, HIPAA presumes the health care professional is acting in good faith in making this determination, if the professional relies on his or her actual knowledge or on credible information from another person who has knowledge or authority. For example, a doctor whose patient has overdosed on opioids is presumed to have complied with HIPAA if, based on talking with or observing the patient, the doctor determines that the patient poses a serious and imminent threat to his or her own health. Even when HIPAA permits this disclosure, however, the disclosure must be consistent with applicable state law and standards of ethical conduct. HIPAA does not preempt any state law or professional ethics standards that would prevent a health care professional from sharing protected health information in the circumstances described here. For example, the doctor in this situation still may be subject to a state law that prohibits sharing information related to mental health or a substance use disorder without the patient’s consent in all circumstances, even if HIPAA would permit the disclosure.

If an adult patient who may pose a danger to self stops coming to psychotherapy sessions and does not respond to attempts to make contact, does HIPAA permit the therapist to contact a family member to check on the patient's well-being even if the patient has told the therapist that they do not want information shared with that person?

Answer:

Yes, under two possible circumstances:

1. Given that the patient is no longer present, if the therapist determines, based on professional judgment, that there may be an emergency situation and that contacting the family member of the absent patient is in the patient’s best interests; or
2. If the disclosure is needed to lessen a serious and imminent threat and the family member is in a position to avert or lessen the threat.

In making the determination about the patient’s best interests, the provider may take into account the patient’s prior expressed preferences regarding disclosures of their information, if any, as well as the circumstances of the current situation. In either case, the health care provider may share or discuss only the information that the family member involved needs to know about the patient’s care or payment for care or the minimum necessary for the purpose of preventing or lessening the threatened harm.

Additionally, if the family member is a personal representative of the patient, the therapist may contact that person. However, a provider may decide not to treat someone as a personal representative if the provider believes that the patient has been or may be subject to violence, abuse, or neglect by the personal representative, or the patient may be endangered by treating the person as the personal representative; and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the person as the personal representative. See 45 CFR 164.502(g)(5).

When does HIPAA allow a hospital to notify an individual’s family, friends, or caregivers that a patient who has been hospitalized for a psychiatric hold has been admitted or discharged?

Answer:

Hospitals may notify family, friends, or caregivers of a patient in several circumstances:

* **When the patient has a personal representative**

A hospital may notify a patient’s personal representative about their admission or discharge and share other PHI with the personal representative without limitation. However, a hospital is permitted to refuse to treat a person as a personal representative if there are safety concerns associated with providing the information to the person, or if a health care professional determines that disclosure is not in the patient’s best interest.
* **When the patient agrees or does not object to family involvement**

A hospital may notify a patient’s family, friends, or caregivers if the patient agrees, or doesn’t object, or if a health care professional is able to infer from the surrounding circumstances, using professional judgment that the patient does not object. This includes when a patient’s family, friends, or caregivers have been involved in the patient’s health care in the past, and the individual did not object.
* **When the patient becomes unable to agree or object and there has already been family involvement**

When a patient is not present or cannot agree or object because of some incapacity or emergency, a health care provider may share relevant information about the patient with family, friends, or others involved in the patient’s care or payment for care if the health care provider determines, based on professional judgment, that doing so is in the best interest of the patient.

For example, a psychiatric hospital may determine that it is in the best interests of an incapacitated patient to initially notify a member of their household, such as a parent, roommate, sibling, partner, or spouse, and inform them about the patient’s location and general condition. This may include, for example, notifying a patient’s spouse that the patient has been admitted to the hospital.

If the health care provider determines that it is in the patient’s interest, the provider may share additional information that is directly related to the family member’s or friend’s involvement with the patient’s care or payment for care, after they clarify the person’s level of involvement. For example, a nurse treating a patient may determine that it is in the patient’s best interest to discuss with the patient’s adult child, who is the patient’s primary caregiver, the medications found in a patient’s backpack and ask about any other medications the patient may have at home.

Decision-making incapacity may be temporary or long-term. Upon a patient’s regaining decision-making capacity, health providers should offer the patient the opportunity to agree or object to sharing their health information with involved family, friends, or caregivers.
* **When notification is needed to lessen a serious and imminent threat of harm to the health or safety of the patient or others**

A hospital may disclose the necessary protected health information to anyone who is in a position to prevent or lessen the threatened harm, including family, friends, and caregivers, without a patient’s agreement. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health or safety. For example, a health care provider may determine that a patient experiencing a mental health crisis has ingested an unidentified substance and that the provider needs to contact the patient’s roommate to help identify the substance and provide the proper treatment, or the patient may have made a credible threat to harm a family member, who needs to be notified so he or she can take steps to avoid harm. OCR would not second guess a health care professional’s judgment in determining that a patient presents a serious and imminent threat to their own, or others’, health or safety.

# May a covered entity collect, use, and disclose criminal justice data under HIPAA?

1. Does HIPAA permit health care providers who are HIPAA covered entities to collect criminal justice data, such as data on arrests, jail days, and utilization of 911 services, and link the criminal justice data to their health data, for purposes of improving treatment and care coordination?

HIPAA does not limit the types of data that providers may seek or obtain about individual patients for treatment purposes. Treatment includes “the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.”  45 CFR 164.501.  Other standards, such as professional ethics rules or state law, may address the scope of health care providers’ independent investigations and data collection pertaining to patients.  Once a HIPAA covered provider obtains criminal justice data about an individual for treatment purposes, or otherwise combines the data with its PHI, the data held by the HIPAA covered entity is considered protected health information (PHI) and the HIPAA Rules would apply to protect the data.

1. Is criminal justice data protected health information (PHI) under HIPAA?

In some circumstances, yes.  To the extent that criminal justice data is maintained by a HIPAA covered entity or its business associate and relates to the past, present, or future physical or mental health or condition of an individual or the provision of or payment for health care to an individual, it is PHI.  For example, when a covered health care provider receives criminal justice data, either directly from the individual or from another source, in order to help inform the treatment and services that the provider will provide to that individual, or otherwise links the criminal justice data with its patient information, it is PHI.

1. Does HIPAA permit health care providers to disclose PHI that includes criminal justice data on individuals to other treating providers without obtaining an authorization from the individuals?

Yes, HIPAA permits a covered health care provider to disclose PHI for treatment purposes to other providers without having to first obtain an authorization from the individuals.  This may include the disclosure of PHI for purposes of coordinating an individual’s care with other treatment facilities or emergency medical technicians (EMTs).

1. Does HIPAA permit multiple health care providers who are seeking to collect individuals’ criminal justice data and link it to the individuals’ health data to engage the services of or work with a third-party to do this on their behalf?

Yes. Multiple covered health care providers can contract with a third party to perform data aggregation and linkage services on their behalf, as long as the providers enter into a HIPAA-compliant business associate agreement (BAA) with the third party, and so long as the aggregation is for purposes permitted under HIPAA. (Such third parties are considered to be “business associates” (BAs) under HIPAA and have direct compliance obligations with certain aspects of the HIPAA Rules.) In these cases, the participating providers may enter into one, common business associate agreement with the third party.

The BAA then governs the subsequent uses and disclosures that the BA may make with the data. For example, the BA may be authorized by its BAA to share the PHI on behalf of the participating providers with each other or other providers for treatment purposes, including care coordination, or, subject to certain conditions, for health care operations purposes. For more information on exchanging PHI for treatment or health care operations purposes, please see:

Permitted Uses and Disclosures: Exchange for Treatment

[www.healthit.gov/sites/default/files/exchange\_treatment.pdf](http://www.healthit.gov/sites/default/files/exchange_treatment.pdf)

Permitted Uses and Disclosures: Exchange for Health Care Operations

<https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf>

1. Does HIPAA permit a health care provider to share the PHI of an individual that may include criminal justice data with a law enforcement official who has the individual in custody and is looking to ensure the individual is seen by the proper treatment facility?

A covered entity is permitted to disclose PHI in response to a request by a law enforcement official having lawful custody of an individual if the official represents that such PHI is needed to provide health care to the individual or for the health and safety of the individual. For more information on permitted disclosures to law enforcement under HIPAA, see OCR’s guidance on sharing protected health information with law enforcement:

[http://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html](https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html)

[http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final\_hipaa\_guide\_law\_enforcement.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf)

While HIPAA permits the disclosure of protected health information to law enforcement in these defined circumstances, other Federal and State laws may impose greater restrictions on the release of certain information, such as substance use disorder information, to law enforcement.

1. Does HIPAA permit health care providers to disclose PHI that includes criminal justice data to other public or private-sector entities providing social services (such as housing, income support, job training)?

In specified circumstances, yes. For example:

* A covered entity may disclose PHI for treatment of the individual without having to obtain the authorization of the individual. Treatment includes the coordination of health care or related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party. Thus, health care providers who believe that disclosures to certain social service entities are a necessary component of or may help further the individual’s health care may disclose the minimum necessary PHI to such entities for treatment purposes without the individual’s authorization. For example, a provider may disclose PHI about a patient needing health care supportive housing to a service agency that arranges such services for individuals.
* A covered entity may also disclose PHI to such entities with an authorization signed by the individual. HIPAA permits authorizations that refer to a class of persons who may receive or use the PHI. Thus, providers could in one authorization identify a broad range of social services entities that may receive the PHI if the individual agrees. For example, an authorization could indicate that PHI will be disclosed to “social services providers” for purposes of “housing, public benefits, counseling, and job readiness.”
1. Does HIPAA restrict the ability of law enforcement officials to use or disclose data they maintain on health or mental health indicators to help inform incident response (g., to ensure officers are prepared to stabilize individuals and/or to support diversion)?

In general, no. Most state and local police or other law enforcement agencies are not covered by HIPAA and thus, are not subject to HIPAA’s use and disclosure rules. HIPAA, however, does apply to the disclosure of health information by most health providers to law enforcement. For more information, see OCR’s HIPAA Guide for Law Enforcement at:

[http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final\_hipaa\_guide\_law\_enforcement.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf)

While HIPAA does not generally apply to use or disclosure of the data by law enforcement officials, other Federal and State laws may apply.

1. In the context of pre-arrest diversion, when does HIPAA permit a health care provider to share PHI with a law enforcement official without an individual’s authorization?

**Calls for service dealing with attempted suicide or a mental health complaint.**  Sometimes a family will call 911 for law enforcement response for a family member in a mental health crisis.  Other times, a business owner or a bystander calls to report unusual behavior (which often is an individual in crisis) and responding officers would benefit from knowing if the individual has a mental health condition.  This type of information may enable officers to employ crisis intervention and de-escalation techniques that could reduce the likelihood of injury to both officers and individuals in a mental health crisis.

HIPAA permits a health care provider to share PHI with law enforcement, in conformance with other applicable laws and ethics rules, in order to “prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.”  45 CFR 164.512(j). For example, if an individual makes a credible threat to inflict serious and imminent bodily harm, such as threatening to commit suicide, a provider may share with law enforcement the information needed to intervene. The provider may rely on a credible representation from a person with apparent knowledge of the situation or authority, such as a law enforcement official, when determining that the disclosure permission applies. See: [http://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html](https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html)

**Other general calls:**  An officer is trying to determine whether an individual has a mental illness, substance abuse problem, or both, and needs to gain information about his or her condition in order to decide whether jail, emergency room, or some other program is needed.

If the individual is in lawful custody, a health care provider may disclose PHI to law enforcement pursuant to 45 CFR 164.512(k)(5) if the official represents that the information is needed to provide health care to the individual or  to provide for the individual’s health and safety or the health and safety of the officers.

If the individual is not in lawful custody (see 45 CFR 164.512 (k)(5)), nor is a threat to self or others (see 45 CFR 164.512(j)), these provisions would not apply and the provider would need to obtain an authorization from the individual before disclosing PHI to law enforcement, unless another HIPAA provision applies (e.g., escaped inmate, apprehension of an admitted perpetrator of violent crime, etc.).  See [http://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html](https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html) for additional provisions that may apply depending on the particular situation.

We note that substance use disorder treatment information may be subject to additional protections under 42 CFR part 2.

1. When is an individual, other than an inmate, considered to be within the “lawful custody” of law enforcement for purposes of 45 CFR 164.512(k)(5) of the HIPAA Privacy Rule? Is “lawful custody” limited to arrest and imminent arrest or does it apply to situations where an individual may be under the care or control of an officer, but not under arrest?

For purposes of the scope of permitted disclosures of PHI to law enforcement in custodial situations under 45 CFR 164.512(k)(5), HIPAA does not define the precise boundaries of “other persons in lawful custody.”  As defined in HIPAA at 45 CFR 164.501, the term includes, but is not limited to:  juvenile offenders adjudicated delinquent, non-citizens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.  In addition to these defined situations, lawful custody also includes those situations where an individual is under the care or control of an officer.  This includes instances where an individual has been arrested, as well as situations where the individual has been detained by law enforcement and is not free to go, but is not under formal arrest.  For example, this would include situations when an officer has detained an individual and seeks to determine whether diversion is appropriate.  Lawful custody does not encompass pretrial release, probation, or parole.

1. Does HIPAA restrict a covered entity’s disclosure of PHI for treatment purposes to only those health care providers that are themselves covered by HIPAA?

No.  A covered entity is permitted to disclose PHI for treatment purposes to any health care provider, including those that are not covered by HIPAA.  In addition, HIPAA permits a covered health care provider to disclose PHI for the treatment of an individual to a third party, such as a social service agency, that is involved in the coordination or management of health care of that individual.

# Does HIPAA permit a doctor to contact a patient’s family or law enforcement if the doctor believes that the patient might hurt herself or someone else?

Yes. The Privacy Rule permits a health care provider to disclose necessary information about a patient to law enforcement, family members of the patient, or other persons, when the provider believes the patient presents a serious and imminent threat to self or others. The scope of this permission is described in a [letter to the nation’s health care providers](https://www.hhs.gov/sites/default/files/ocr/office/lettertonationhcp.pdf).

Specifically, when a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others, the Privacy Rule allows the provider, consistent with applicable law and standards of ethical conduct, to alert those persons whom the provider believes are reasonably able to prevent or lessen the threat. These provisions may be found in the Privacy Rule at 45 CFR § 164.512(j).

Under these provisions, a health care provider may disclose patient information, including information from mental health records, if necessary, to law enforcement, family members of the patient, or any other persons who may reasonably be able to prevent or lessen the risk of harm. For example, if a mental health professional has a patient who has made a credible threat to inflict serious and imminent bodily harm on one or more persons, HIPAA permits the mental health professional to alert the police, a parent or other family member, school administrators or campus police, and others who may be able to intervene to avert harm from the threat.

In addition to professional ethical standards, most States have laws and/or court decisions which address, and in many instances require, disclosure of patient information to prevent or lessen the risk of harm. Providers should consult the laws applicable to their profession in the States where they practice, as well as 42 USC 290dd-2 and 42 CFR Part 2 under Federal law (governing the disclosure of alcohol and drug abuse treatment records) to understand their duties and authority in situations where they have information indicating a threat to public safety. Note that, where a provider is not subject to such State laws or other ethical standards, the HIPAA permission still would allow disclosures for these purposes to the extent the other conditions of the permission are met.

# If a law enforcement officer brings a patient to a hospital or other mental health facility to be placed on a temporary psychiatric hold, and requests to be notified if or when the patient is released, can the facility make that notification?

The Privacy Rule permits a HIPAA covered entity, such as a hospital, to disclose certain protected health information, including the date and time of admission and discharge, in response to a law enforcement official’s request, for the purpose of locating or identifying a suspect, fugitive, material witness, or missing person. See 45 CFR § 164.512(f)(2). Under this provision, a covered entity may disclose the following information about an individual: name and address; date and place of birth; social security number; blood type and rh factor; type of injury; date and time of treatment (includes date and time of admission and discharge) or death; and a description of distinguishing physical characteristics (such as height and weight). However, a covered entity may not disclose any protected health information under this provision related to DNA or DNA analysis, dental records, or typing, samples, or analysis of body fluids or tissue. The law enforcement official’s request may be made orally or in writing.

Other Privacy Rule provisions also may be relevant depending on the circumstances, such as where a law enforcement official is seeking information about a person who may not raise to the level of a suspect, fugitive, material witness, or missing person, or needs protected health information not permitted under the above provision. For example, the Privacy Rule’s law enforcement provisions also permit a covered entity to respond to an administrative request from a law enforcement official, such as an investigative demand for a patient’s protected health information, provided the administrative request includes or is accompanied by a written statement specifying that the information requested is relevant, specific and limited in scope, and that de-identified information would not suffice in that situation. The Rule also permits covered entities to respond to court orders and court-ordered warrants, and subpoenas and summonses issued by judicial officers. See 45 CFR § 164.512(f)(1). Further, to the extent that State law may require providers to make certain disclosures, the Privacy Rule would permit such disclosures of protected health information as “required-by-law” disclosures. See 45 CFR § 164.512(a).

Finally, the Privacy Rule permits a covered health care provider, such as a hospital, to disclose a patient’s protected health information, consistent with applicable legal and ethical standards, to avert a serious and imminent threat to the health or safety of the patient or others. Such disclosures may be to law enforcement authorities or any other persons, such as family members, who are able to prevent or lessen the threat. See 45 CFR § 164.512(j).

# If a doctor believes that a patient might hurt himself or herself or someone else, is it the duty of the provider to notify the family or law enforcement authorities?

A health care provider’s “duty to warn” generally is derived from and defined by standards of ethical conduct and State laws and court decisions such as Tarasoff v. Regents of the University of California. HIPAA permits a covered health care provider to notify a patient’s family members of a serious and imminent threat to the health or safety of the patient or others if those family members are in a position to lessen or avert the threat. Thus, to the extent that a provider determines that there is a serious and imminent threat of a patient physically harming self or others, HIPAA would permit the provider to warn the appropriate person(s) of the threat, consistent with his or her professional ethical obligations and State law requirements. See 45 CFR 164.512(j). In addition, even where danger is not imminent, HIPAA permits a covered provider to communicate with a patient’s family members, or others involved in the patient’s care, to be on watch or ensure compliance with medication regimens, as long as the patient has been provided an opportunity to agree or object to the disclosure and no objection has been made. See 45 CFR 164.510(b)(2).

Does HIPAA require a mental health provider to let a patient know that the provider is going to share information with others before disclosing PHI to prevent or lessen a serious and imminent threat?

Answer:

Not at the time of disclosure; however, the Notice of Privacy Practices should contain an example of this type of disclosure so patients are informed in advance of that possibility. See 45 CFR 164.520(b). In situations that also involve reports to the appropriate government authority that the patient may be an adult victim of abuse, neglect, or domestic violence, the mental health provider must promptly inform the patient that a report has been or will be made, unless:

* informing the patient would create a danger to the patient; or
* the provider would be informing a personal representative, and the provider reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the patient is determined by the provider, in the exercise of professional judgment. See 45 CFR 164.512(c).

Other standards, such as clinical protocols, ethics rules, or state laws, may also be applicable to patient notification about disclosures in situations involving threats of imminent harm.

# How does HIPAA interact with the federal confidentiality rules for substance use disorder treatment information in an emergency situation—which rules should be followed?

### Answer:

A health provider that provides treatment for substance use disorders, including opioid abuse, needs to determine whether it is subject to 42 CFR Part 2 (i.e., a “Part 2 program”) and whether it is a covered entity under HIPAA. Generally, the Part 2 rules provide more stringent privacy protections than HIPAA, including in emergency situations. If an entity is subject to both Part 2 and HIPAA, it is responsible for complying with the more protective Part 2 rules, as well as with HIPAA. HIPAA is intended to be a set of minimum federal privacy standards, so it generally is possible to comply with HIPAA and other laws, such as 42 CFR Part 2, that are more protective of individuals’ privacy.

For example, HIPAA permits disclosure of protected health information (PHI) for treatment purposes (including in emergencies) without patient authorization, and allows PHI to be used or disclosed to lessen a threat of serious and imminent harm to the health or safety of the patient or others (which may occur as part of a health emergency) without patient authorization or permission. Because HIPAA permits, but does not require, disclosures for treatment or to prevent harm, if Part 2 restricts certain disclosures during an emergency, an entity subject to both sets of requirements could comply with Part 2’s restrictions without violating HIPAA.

# Does HIPAA provide extra protections for mental health information compared with other health information?

Generally, the Privacy Rule applies uniformly to all protected health information, without regard to the type of information. One exception to this general rule is for psychotherapy notes, which receive special protections. The Privacy Rule defines psychotherapy notes as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient’s medical record. Psychotherapy notes do not include any information about medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, or results of clinical tests; nor do they include summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date. Psychotherapy notes also do not include any information that is maintained in a patient’s medical record. See 45 CFR 164.501.

Psychotherapy notes are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for treatment, payment, or health care operations purposes, other than by the mental health professional who created the notes. Therefore, with few exceptions, the Privacy Rule requires a covered entity to obtain a patient’s authorization prior to a disclosure of psychotherapy notes for any reason, including a disclosure for treatment purposes to a health care provider other than the originator of the notes. See 45 CFR 164.508(a)(2). A notable exception exists for disclosures required by other law, such as for mandatory reporting of abuse, and mandatory “duty to warn” situations regarding threats of serious and imminent harm made by the patient (State laws vary as to whether such a warning is mandatory or permissible).

# What constitutes a “serious and imminent” threat that would permit a health care provider to disclose PHI to prevent harm to the patient, another person, or the public without the patient’s authorization or permission?

### Answer:

HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health or safety posed by a patient. OCR would not second guess a health professional’s good faith belief that a patient poses a serious and imminent threat to the health or safety of the patient or others and that the situation requires the disclosure of patient information to prevent or lessen the threat. Health care providers may disclose the necessary protected health information to anyone who is in a position to prevent or lessen the threatened harm, including family, friends, caregivers, and law enforcement, without a patient’s permission.

# What options do family members of an adult patient with mental illness have if they are concerned about the patient’s mental health and the patient refuses to agree to let a health care provider share information with the family?

The HIPAA Privacy Rule permits a health care provider to disclose information to the family members of an adult patient who has capacity and indicates that he or she does not want the disclosure made, only to the extent that the provider perceives a serious and imminent threat to the health or safety of the patient or others and the family members are in a position to lessen the threat. Otherwise, under HIPAA, the provider must respect the wishes of the adult patient who objects to the disclosure. However, HIPAA in no way prevents health care providers from listening to family members or other caregivers who may have concerns about the health and well-being of the patient, so the health care provider can factor that information into the patient’s care.

In the event that the patient later requests access to the health record, any information disclosed to the provider by another person who is not a health care provider that was given under a promise of confidentiality (such as that shared by a concerned family member), may be withheld from the patient if the disclosure would be reasonably likely to reveal the source of the information. 45 CFR 164.524(a)(2)(v). This exception to the patient’s right of access to protected health information gives family members the ability to disclose relevant safety information with health care providers without fear of disrupting the family’s relationship with the patient.

# Does HIPAA prevent a school administrator, or a school doctor or nurse, from sharing concerns about a student’s mental health with the student’s parents or law enforcement authorities?

Student health information held by a school generally is subject to the Family Educational Rights and Privacy Act (FERPA), not HIPAA. HHS and the Department of Education have developed [guidance clarifying the application of HIPAA and FERPA](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf).

In the limited circumstances where the HIPAA Privacy Rule, and not FERPA, may apply to health information in the school setting, the Rule allows disclosures to parents of a minor patient or to law enforcement in various situations. For example, parents generally are presumed to be the personal representatives of their unemancipated minor child for HIPAA privacy purposes, such that covered entities may disclose the minor’s protected health information to a parent. See 45 CFR § 164.502 (g)(3). In addition, disclosures to prevent or lessen serious and imminent threats to the health or safety of the patient or others are permitted for notification to those who are able to lessen the threat, including law enforcement, parents or others, as relevant. See 45 CFR § 164.512(j).

Does HIPAA permit health care providers to share protected health information (PHI) about an individual who has mental illness with other health care providers who are treating the same individual for care coordination/continuity of care purposes?

Answer:

HIPAA permits health care providers to disclose to other health providers any protected health information (PHI) contained in the medical record about an individual for treatment, case management, and coordination of care and, with few exceptions, treats mental health information the same as other health information. Some examples of the types of mental health information that may be found in the medical record and are subject to the same HIPAA standards as other protected health information include:

* medication prescription and monitoring
* counseling session start and stop times
* the modalities and frequencies of treatment furnished
* results of clinical tests
* summaries of: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

HIPAA generally does not limit disclosures of PHI between health care providers for treatment, case management, and care coordination, except that covered entities must obtain individuals’ authorization to disclose separately maintained psychotherapy session notes for such purposes. Covered entities should determine whether other rules, such as state law or professional practice standards place additional limitations on disclosures of PHI related to mental health.

Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes? For example, can a health care provider refer a homeless patient to a social services agency, such as a housing provider, when doing so may reveal that the basis for eligibility is related to mental health?

Answer:

HIPAA, with few exceptions, treats all health information, including mental health information, the same. HIPAA allows health care providers to disclose protected health information (PHI), including mental health information, to other public or private-sector entities providing social services (such as housing, income support, job training) in specified circumstances.  For example:

* A health care provider may disclose a patient’s PHI for treatment purposes without having to obtain the authorization of the individual. Treatment includes the coordination or management of health care by a health care provider with a third party. Health care means care, services, or supplies related to the health of an individual. Thus, health care providers who believe that disclosures to certain social service entities are a necessary component of, or may help further, the individual’s health or mental health care may disclose the minimum necessary PHI to such entities without the individual’s authorization. For example, a provider may disclose PHI about a patient needing mental health care supportive housing to a service agency that arranges such services for individuals.
* A covered entity may also disclose PHI to such entities pursuant to an authorization signed by the individual. HIPAA permits authorizations that refer to a class of persons who may receive or use the PHI. Thus, providers could in one authorization identify a broad range of social services entities that may receive the PHI if the individual agrees. For example, an authorization could indicate that PHI will be disclosed to “social services providers” for purposes of “supportive housing, public benefits, counseling, and job readiness.”

# How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

The HIPAA Privacy Rule requires a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the Rule requires covered entities to make their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.

The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.

# Won't the HIPAA Privacy Rule's minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?

### Answer:

No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements.

Uses of protected health information for treatment are not exempt from the minimum necessary standard. However, the Privacy Rule provides the covered entity with substantial discretion with respect to how it implements the minimum necessary standard, and appropriately and reasonably limits access to identifiable health information within the covered entity. The Rule recognizes that the covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity may develop role-based access policies that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

# Do the HIPAA Privacy Rule's minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patient medical information in the course of their training?

### Answer:

No. The definition of “health care operations” in the Privacy Rule provides for “conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers.” [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients’ medical information, including entire medical records.

# Must the HIPAA Privacy Rule's minimum necessary standard to be applied to uses or disclosures that are authorized by an individual?

### Answer:

No. Uses and disclosures that are authorized by the individual are exempt from the minimum necessary requirements. For example, if a covered health care provider receives an individual’s authorization to disclose medical information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The authorization must meet the requirements of [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml).

# Are providers required to make a minimum necessary determination to disclose to Federal or state agencies, such as the Social Security Administration (SSA) or its affiliated agencies, for individuals' applications for federal or state benefits?

### Answer:

No. These disclosures must be authorized by an individual and, therefore, are exempt from the HIPAA Privacy Rule’s minimum necessary requirements. Furthermore, use of the provider’s own authorization form is not required. Providers can accept an agency’s authorization form as long as it meets the requirements of [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml) of the Privacy Rule.

# Doesn't the HIPAA Privacy Rule minimum necessary standard conflict with the HIPAA transaction standards?

### Answer:

No, because the Privacy Rule exempts from the minimum necessary standard any uses or disclosures that are required for compliance with the applicable requirements of the transactions standards, including disclosures of all data elements that are required or situationally required in those transactions. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(b)(2)(vi).

However, [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) have significant discretion as to the information included in the transactions as optional data elements. Therefore, the minimum necessary standard does apply to the optional data elements. The transactions standard adopted for the outpatient pharmacy sector is an example of a standard that uses optional data elements. The health plan, or payer, currently specifies which of the optional data elements are needed for payment of its particular pharmacy claims. The health plan or its business associates must apply the minimum necessary standard when requesting this information. In this example, a pharmacist may reasonably rely on the health plan’s request for information as the minimum necessary for the intended disclosure. For example, as part of a routine protocol, the name of the individual may be requested by the payer as the minimum necessary to validate the identity of the claimant or for drug interaction or other patient safety reasons.

# Does the HIPAA Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time the entire medical record is disclosed?

### Answer:

No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may use, disclose, or request an entire medical record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.

For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures and requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes.The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment purposes or disclosures to the individual who is the subject of the protected health information.

# A provider might have a patient's medical record that contains older portions of a medical record that were created by another previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

### Answer:

Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

# In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigning office space and upgrading computer systems, in order to comply with the HIPAA Privacy Rule's minimum necessary requirements?

### Answer:

No. The basic standard for minimum necessary uses requires that [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) make reasonable efforts to limit access to protected health information to those in the workforce that need access based on their roles in the covered entity.

The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Covered entities should also take into account their ability to configure their record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small, solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. In this case, appropriate training of employees may be sufficient. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the Privacy Rule.

# Is a covered entity required to apply the HIPAA Privacy Rule's minimum necessary standard to a disclosure of protected health information it makes to another covered entity?

### Answer:

Covered entities are required to apply the minimum necessary standard to their own requests for protected health information. One covered entity may reasonably rely on another covered entity’s request as the minimum necessary, and then does not need to engage in a separate minimum necessary determination. See [45 CFR 164.514(d)(3)(iii)](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml).

However, if a covered entity does not agree that the amount of information requested by another covered entity is reasonably necessary for the purpose, it is up to both covered entities to negotiate a resolution of the dispute as to the amount of information needed. Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with another covered entity making a request, and negotiating an information exchange that meets the needs of both parties. Such discussions occur today and may continue after the compliance date of the Privacy Rule.

# May a covered entity accept documentation of an external Institutional Review Board's (IRB) waiver of authorization for purposes of reasonably relying on the request as the minimum necessary?

### Answer:

Yes. The HIPAA Privacy Rule explicitly permits a covered entity to reasonably rely on a researcher’s documentation of an Institutional Review Board (IRB) or Privacy Board waiver of authorization pursuant to [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(i) that the information requested is the minimum necessary for the research purpose. See 45 CFR 164.514(d)(3)(iii). This is true regardless of whether the documentation is obtained from an external IRB or Privacy Board or from one that is associated with the covered entity.

# Are hospitals or other health care providers required to provide their notices to patients they treat in an emergency?

### Answer:

Hospitals and other covered health care providers with a direct treatment relationship with individuals are not required to provide their notices to patients at the time they are providing emergency treatment. In these situations, the HIPAA Privacy Rule requires only that providers give patients a notice when it is practical to do so after the emergency situation has ended. In addition, where notice is delayed by an emergency treatment situation, the Privacy Rule does not require that providers make a good faith effort to obtain the patient’s written acknowledgment of receipt of the notice.

# If a health care provider chooses to obtain an individual's consent to use or disclose protected health information about them, does the provider also have to make a good faith effort to obtain the individual's acknowledgement of the notice?

### Answer:

Yes. The HIPAA Privacy Rule requires that a covered health care provider with a direct treatment relationship with individuals make a good faith effort to obtain written acknowledgments from those individuals that they have received the provider’s notice, regardless of whether the provider also chooses to obtain the individuals’ consent. However, those providers that choose to obtain consent from individuals have discretion to design one form that includes both a consent and the acknowledgment of receipt of the notice.

# Does the HIPAA Privacy Rule require a health care provider to obtain a new acknowledgement of receipt of the notice from patients if the facility changes its privacy policy?

### Answer:

No. A covered health care provider with a direct treatment relationship with individuals is required to make a good faith effort to obtain an individual's acknowledgement of receipt of the notice only at the time the provider first gives the notice to the individual -- that is, at first service delivery. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c)(2).

# Does the HIPAA Privacy Rule permit health care providers to obtain an electronic acknowledgement of the notice from individuals?

### Answer:

Yes. For notice delivered electrically, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice. A provider who gives his paper notice to a patient during a face-to-face encounter with the individual at first service delivery may also obtain an electronic acknowledgment from the individual, provided that the individual’s acknowledgment is in writing. Thus, a receptionist’s notation in the provider’s computer system of the individual’s receipt of the notice would not be considered a valid written acknowledgment of the individual.

# Are covered entities permitted to give individuals a “layered” notice?

### Answer:

Yes. Covered entities may use a “layered” notice to implement the HIPAA Privacy Rule’s requirements, so long as the elements required by [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(b) are included in the document that is provided to the individual. For example, a covered entity may satisfy the notice requirements by providing the individual with both a short notice that briefly summarizes the individual’s rights, as well as other information; and a longer notice, layered beneath the short notice, that contains all of the elements required by the Privacy Rule. Providing the notice in this fashion is a helpful tool to assure that more individuals will realize that important information is contained in the notice. In addition to ensuring the notice is in plain language (as required by the Privacy Rule), [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) are encouraged to develop notices that maximize readability and clarity.

# Are health plans required to make a good faith effort to obtain from their enrollees a written acknowledgement of receipt of the notice?

### Answer:

No. Under the HIPAA Privacy Rule, only covered health care providers that have a direct treatment relationship with individuals are required to make a good faith effort to obtain the individual's acknowledgment of receipt of the notice. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c)(2)(ii).

# How are health care providers supposed to provide the notice to individuals and obtain their written acknowledgement of the notice when the first treatment encounter is over the phone or in some other manner that is not face-to-face?

### Answer:

The HIPAA Privacy Rule is intended to be flexible enough to address the various types of relationships that covered health care providers may have with the individuals they treat, including those treatment situations that are not face-to-face. For example, a health care provider who first treats a patient over the phone satisfies the notice provision requirements of the Privacy Rule by mailing the notice to the individual the same day, if possible. To satisfy the requirement that the provider also make a good faith effort to obtain the individual’s acknowledgment of the notice, the provider may include a tear-off sheet or other document with the notice that requests that the acknowledgment be mailed back to the provider. The health care provider is not in violation of the Rule if the individual chooses not to mail back an acknowledgment; and a file copy of the form sent to the patient would be adequate documentation of the provider’s good faith effort to obtain the acknowledgment.

Where a health care provider’s initial contact with the patient is simply to schedule an appointment or a procedure, the notice provision and acknowledgment requirements may be satisfied at the time the individual arrives at the provider’s facility for his or her appointment.

For service provided electronically, the notice must be sent electronically automatically and contemporaneously in response to the individual’s first request for service. In this situation, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice.

# We participate in an organized health care arrangement (OHCA). How are we to comply with the HIPAA Privacy Rule's requirements for providing notices and obtaining individuals' acknowledgements of the notice?

### Answer:

Health care providers and other [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) that participate in an organized health care arrangement (OHCA) may use a single, joint notice that covers all of the participating covered entities (provided that the conditions at [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(d) are met), or may each maintain separate notices. Where a joint notice is provided to an individual by any one of the covered entities to which the joint notice applies, the Privacy Rule’s requirements for providing the notice are satisfied for all others covered by the joint notice. If the joint notice is provided to an individual by a direct treatment provider participating in the OHCA, the provider must make a good faith effort to obtain the individual’s written acknowledgment of receipt of the joint notice. Where the joint notice is provided to the individual by a participating covered entity other than a direct treatment provider, no acknowledgment need be obtained.

However, where covered entities participating in an OHCA choose to maintain separate notices, each covered entity from which an individual obtains services must provide its notice to the individual in accordance with the applicable requirements of 45 CFR 164.520(c). In addition, each direct treatment provider within the OHCA must make a good faith effort to obtain the individual’s acknowledgment of the notice he or she provides.

# Does a health plan have to provide a copy of its notice to each dependent receiving coverage under a policy?

### Answer:

No. A health plan satisfies the HIPAA Privacy Rule’s requirements for providing the notice by distributing its notice only to the named insured of a policy under which coverage is provided both to the named insured and his or her dependents. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c)(1)(iii).

# For group health plan products, can the health plan send its notice to the administrator of the group product or the plan sponsor for them to distribute to each employee enrolled in the plan?

### Answer:

The HIPAA Privacy Rule requires a health plan to distribute its notice to each individual covered by the plan. Health plans may arrange to have another person or entity, for example, a group administrator or a plan sponsor, distribute the notice on their behalf. However, if the other person or entity fails to distribute the notice to the plan’s enrollees, the health plan may be in violation of the Privacy Rule.

# As a pediatrician, am I required to give my notice of privacy practices to the children I treat?

### Answer:

The HIPAA Privacy Rule requires a covered health care provider with a direct treatment relationship with the individual to provide the notice to the individual receiving treatment no later than the date of first service delivery. In cases where the individual has a personal representative, as is generally the case when a parent brings a child in for treatment, the provider satisfies the notice distribution requirements by providing the notice to the personal representative (e.g., the child’s parent), and making a good faith effort to obtain the personal representative’s acknowledgment of the notice.

In the limited cases where the parent is not the personal representative of the unemancipated minor, such as when the minor is authorized under State law to consent to the treatment and does so, the provider must give its notice to the minor and make a good faith effort to obtain the minor's acknowledgment of the notice. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(g)(3) and [164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c)(2).

# Are health care providers required by the HIPAA Privacy Rule to post their entire notice at their facility or may they post just a brief description of the notice?

### Answer:

Covered health care providers that maintain an office or other physical site where they provide health care directly to individuals are required to post their entire notice at the facility in a clear and prominent location. The Privacy Rule, however, does not prescribe any specific format for the posted notice, just that it include the same information that is distributed directly to the individual. Covered health care providers have discretion to design the posted notice in a manner that works best for their facility, which may be to simply post a copy of the pages of the notice that is provided directly to individuals.

# Can a covered entity bypass obtaining an individual's authorization for a use or disclosure not permitted by the HIPAA Privacy Rule simply by informing individuals of the use or disclosure through it notice of privacy practices?

### Answer:

No. A covered entity’s notice is not a substitute for an individual’s authorization. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) are required to obtain the individual’s written authorization for any use or disclosure of protected health information not permitted or required by the Privacy Rule. See [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml). Simply including in the notice a description of such a use or disclosure does not obviate the need for the covered entity to obtain the individual’s prior written authorization, when that authorization is required by the Rule. Instead, the notice must reflect the uses and disclosures a covered entity may make without the individual’s authorization, as permitted by Privacy Rule, as well as state that any other uses or disclosures only will be made with the individual’s written authorization. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(b).

# Is our medical practice required to notify patients through the mail of any changes to our notice?

### Answer:

No. The HIPAA Privacy Rule does not require a covered health care provider to mail out its revised notice or otherwise notify patients by mail of changes to the notice. Rather, when a covered health care provider with a direct treatment relationship with individuals makes a change to his notice, he must make the notice available upon request to patients or other persons on or after the effective date of the revision, and, if he maintains a physical service delivery site, post the revised notice in a clear and prominent location in his facility. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c)(2)(iv). In addition, the provider must ensure that the current notice, in effect at that time, is provided to patients at first service delivery, and made available on his customer service web site, if he has one. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c).

# Is a physician required to give her notice to every patient or can she just post the notice in her waiting room and give a copy to those patients who ask for it?

### Answer:

The HIPAA Privacy Rule requires a covered health care provider with direct treatment relationships with individuals to give the notice to every individual no later than the date of first service delivery to the individual and to make a good faith effort to obtain the individual’s written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where she provides health care directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(c) for other notice provision requirements.

# It is common for hospitals and other health care providers to collect preoperative information over the phone from a new patient prior to the day of surgery in order to determine whether the patient has any special medical concerns or issues that need to be addressed. Does the HIPAA Privacy Rule prohibit this practice if the patient has not yet received or acknowledged the provider's notice?

### Answer:

No, the Privacy Rule does not prohibit this practice. Where a health care provider’s initial contact with a patient is simply to schedule an appointment or a procedure, or to collect information in anticipation of an appointment or a procedure, the Privacy Rule’s requirements for providing the notice and obtaining a patient’s acknowledgment of the notice may be satisfied at the time the individual arrives at the provider’s facility for his or her appointment or procedure.

# Is a pharmacist permitted to have a customer acknowledge receipt of the notice by signing or initialing the log book that they already sign when they pick up prescriptions?

### Answer:

Yes, provided that the individual is clearly informed on the log book of what they are acknowledging and the acknowledgment is not also used as a waiver or permission for something else that also appears on the log book (such as a waiver to consult with the pharmacist). The HIPAA Privacy Rule provides covered health care providers with discretion to design an acknowledgment process that works best for their businesses.

# Must a covered entity with a Notice of Privacy Practices that reflects more stringent state laws of multiple states, revise the whole Notice every time one state law materially changes?

### Answer:

The Privacy Rule requires the Notice of Privacy Practices (Notice) to identify, among other things, what uses and disclosures the covered entity may make of protected health information. The Notice must reflect any State law(s) that is more stringent than the Privacy Rule with respect to the use or disclosure of this information. Where the covered entity is subject to the privacy laws of multiple States, the more stringent use and disclosure laws of each of the States, if any, must be reflected in the Notice. See [45 CFR 164.520](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-520.xml)(b)(1)(ii)(C).

When there is a material revision to the Notice based on a change in State law, covered entities must use the revised Notice to meet the Rule’s requirements for distribution of the Notice that occur on or after the effective date of the revised Notice. See, generally, §§164.520(c)(1)-(3). In particular, a health plan must provide individuals (in most cases, the named insured) then covered by the plan with the revised Notice within 60 days of the revision. See §164.520(c)(1)(i)(C).

The Notice requirements are intended to ensure that individuals are fairly informed about how a covered entity may use or disclose their personal health information, including important limitations imposed by State law. Although a covered entity can describe more stringent State privacy laws in the uses and disclosures section of its Notice, this may be more confusing than informative to the individual, particularly where multiple and varying State laws may be applicable. There are other ways a covered entity can design its Notice that may make this information easier for the individual to read and understand, as well as to facilitate the covered entity’s ability to keep the information current and accurate. For instance, a general statement could be included in the uses and disclosures section of the Notice that clearly identifies and refers the reader to a separate section of the Notice which describes the more stringent State privacy law(s) and more fully informs the reader about how protected health information may be used and disclosed. Thus, when more stringent State privacy laws materially change the covered entity’s privacy practices, the covered entity would need to revise only the section of the Notice that contains the State law specific information.

Having a separable section on more stringent State laws can also facilitate distribution of the revised Notice when material changes occur in this section of the Notice. The revised State law section, if on a separate page, may be more readily inserted in or associated with existing Notices in place of the out-dated material.

# Does the HIPAA Privacy Rule change the way in which a person can grant another person health care power of attorney?

### Answer:

No. Nothing in the Privacy Rule changes the way in which an individual grants another person power of attorney for health care decisions. State law (or other law) regarding health care powers of attorney continue to apply. The intent of the provisions regarding personal representatives was to complement, not interfere with or change, current practice regarding health care powers of attorney or the designation of other personal representatives. Such designations are formal, legal actions which give others the ability to exercise the rights of, or make treatment decisions related to, an individual. The Privacy Rule provisions regarding personal representatives generally grant persons, who have authority to make health care decisions for an individual under other law, the ability to exercise the rights of that individual with respect to health information.

# If someone has a health care power of attorney for an individual, can they obtain access to that individual's medical record?

### Answer:

Yes, an individual that has been given a health care power of attorney will have the right to access the medical records of the individual related to such representation to the extent permitted by the HIPAA Privacy Rule at [45 CFR 164.524](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-524.xml).

However, when a physician or other covered entity reasonably believes that an individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse or neglect by the personal representative, or that treating a person as an individual’s personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual’s personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual.

# Does the HIPAA Privacy Rule address when a person may not be the appropriate person to control an individual's protected health information?

### Answer

Generally, no. The Rule defers to State and other laws that address the fitness of a person to act on an individual’s behalf. However, a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) does not have to treat a personal representative as the individual when it reasonably believes, in the exercise of professional judgment, the individual is subject to domestic violence, abuse or neglect by the personal representative, or doing so would otherwise endanger the individual.

# May personal representatives access health information based on a non-health care power of attorney?

### Answer:

No. Except with respect to decedents, a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) must treat a personal representative as the individual only when that person has authority under other law to act on the individual’s behalf on matters related to health care. A power of attorney that does not include decisions related to health care in its scope would not authorize the holder to exercise the individual’s rights under the HIPAA Privacy Rule. Further, a covered entity does not have to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

With respect to personal representatives of deceased individuals, the Privacy Rule requires a covered entity to treat the personal representative as the individual as long as the person has the authority under law to act for the decedent or the estate. The power of attorney would have to be valid after the individual’s death to qualify the holder as the personal representative of the decedent.

# May adults with mental retardation control their protected health information if they are able to authorize uses and disclosures of their protected health information?

### Answer:

Individuals may control their protected health information under the HIPAA Privacy Rule to the extent State or other law permits them to act on their own behalf. Further, even if an individual is deemed incompetent under State or other law to act on his or her own behalf, [covered entities](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) may decline a request by a personal representative for protected health information if the individual objects to the disclosure (or for any other reason), and the disclosure is merely permitted, but not required, under the Rule.

However, covered entities must make disclosures that are required under the Rule (i.e., disclosures to the Secretary under subpart C of part 160 regarding enforcement of the Rule, and to the individual under [45 CFR 164.524](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-524.xml) and [164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml) with respect to the individual’s right of access to his or her protected health information and an accounting of disclosures, respectively). Consequently, with respect to the individual’s right of access to protected health information and for an accounting of disclosures, covered entities must provide the individual’s personal representative access to the individual’s protected health information or an accounting of disclosures upon the request of the personal representative, unless the covered entity, in the exercise of professional judgment, believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. The Rule allows a specified time period before a covered entity must act on such a request; and during this interim period, an individual and his personal representative will have an opportunity to resolve any dispute they may have concerning the request.

# How does a covered entity identify an individual’s personal representative?

### Answer:

State or other law determines who is authorized to act on an individual’s behalf, thus the Privacy Rule does not address how personal representatives should be identified. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) should continue to identify personal representatives the same way they have in the past. However, the HIPAA Privacy Rule does require covered entities to verify a personal representative’s authority in accordance with [45 CFR 164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(h).

# If a child receives emergency medical care without a parent's consent, can the parent get all information about the child's treatment and condition?

### Answer:

Generally, yes. Even though the parent did not consent to the treatment in this situation, the parent would be the child’s personal representative under the HIPAA Privacy Rule. This would not be so when the parent does not have authority to act for the child (e.g., parental rights have been terminated), when expressly prohibited by State or other applicable law, or when the covered entity, in the exercise of professional judgment, believes that providing such information would not be in the best interest of the individual because of a reasonable belief that the individual may be subject to abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

# Does the HIPAA Privacy Rule provide rights for children to be treated without parental consent?

### Answer:

No. The Privacy Rule does not address consent to treatment, nor does it preempt or change State or other laws that address consent to treatment. The Rule addresses access to, and disclosure of, health information, not the underlying treatment.

# Does the HIPAA Privacy Rule preempt state laws?

### Answer:

The HIPAA Privacy Rule provides a Federal floor of privacy protections for individuals' individually identifiable health information where that information is held by a covered entity or by a business associate of the [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp). State laws that are contrary to the Privacy Rule are preempted by the Federal requirements, unless a specific exception applies. These exceptions include if the State law:

1. relates to the privacy of individually identifiable health information and provides greater privacy protections or privacy rights with respect to such information,
2. provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or
3. requires certain health plan reporting, such as for management or financial audits. In these circumstances, a covered entity is not required to comply with a contrary provision of the Privacy Rule.

In addition, the Department of Health and Human Services (HHS) may, upon specific request from a State or other entity or person, determine that a provision of State law which is "contrary" to the Federal requirements – as defined by the HIPAA Administrative Simplification Rules – and which meets certain additional criteria, will not be preempted by the Federal requirements. Thus, preemption of a contrary State law will not occur if the Secretary or designated HHS official determines, in response to a request, that one of the following criteria apply: the State law:

1. is necessary to prevent fraud and abuse related to the provision of or payment for health care,
2. is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation,
3. is necessary for State reporting on health care delivery or costs,
4. is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
5. has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

It is important to recognize that only State laws that are "contrary" to the Federal requirements are eligible for an exemption determination. As defined by the Administrative Simplification Rules, contrary means that it would be impossible for a covered entity to comply with both the State and Federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.

# How does the HIPAA Privacy Rule reduce the potential for conflict with state laws?

### Answer:

The Privacy Rule is designed to minimize conflicts between Federal requirements and those of State law in the following ways:

- The Privacy Rule establishes a floor of Federal privacy protections and individual rights with respect to individually identifiable health information held by covered entities and their business associates. Covered entities may provide greater privacy rights to individuals and greater protections on such information. In addition, covered entities may comply with State laws that provide greater protections for individually identifiable health information and greater privacy rights for individuals.

- The Privacy Rule permits a covered entity to use or disclose protected health information if a State law requires the use or disclosure. See 45 C.F.R. 164.512(a).

- The Privacy Rule permits a covered entity to disclose protected health information to a public health authority who is authorized by law to collect such information for the purposes of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions. (See 45 C.F.R. 164.512(b) for all of the public health disclosures permitted by the Privacy Rule.) Thus, State laws that provide for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation, or intervention, likely will not conflict with the Privacy Rule. In the unusual case where there is a conflict, the State law would stand. See 45 C.F.R. 160.203(c). Because the Administrative Simplification Rules themselves exempt such State laws from preemption, a request for the Department of Health and Human Services (HHS) to issue a preemption exception determination is unnecessary and inappropriate.

- The Privacy Rule permits a covered entity to disclose protected health information to a health oversight agency for oversight activities authorized by law, such as audits and licensure activities. See 45 C.F.R. 164.512(d). Thus, State laws that provide for certain health plan reporting for the purpose of management or financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals, likely will not conflict with the Privacy Rule. In the unusual case where there is a conflict, the State law would stand. See 45 C.F.R. 160.203(d). Because the Administrative Simplification Rules themselves exempt such State laws from preemption, a request for the Department of Health and Human Services (HHS) to issue a preemption exception determination is unnecessary and inappropriate.

# How do I know if a state law is "contrary" to the HIPAA Privacy Rule?

### Answer:

A State law is "contrary" to the HIPAA Privacy Rule if it would be impossible for a covered entity to comply with both the State law and the Federal Privacy Rule requirements, or if the State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. See the definition of "contrary" at 45 C.F.R. 160.202.

For example, a State law that prohibits the disclosure of protected health information to an individual who is the subject of the information may be contrary to the Privacy Rule, which requires the disclosure of protected health information to an individual in certain circumstances. With certain exceptions, the Privacy Rule preempts "contrary" State laws. See 45 C.F.R. Part 160, Subpart B.  [View an unofficial version of the Privacy Rule and the preemption requirements.](https://www.hhs.gov/sites/default/files/adminsimpregtext.pdf)

# How do I know if a state law is "more stringent" than the HIPAA Privacy Rule?

### Answer:

In general, a State law is "more stringent" than the HIPAA Privacy Rule if it relates to the privacy of individually identifiable health information and provides greater privacy protections for individuals' identifiable health information, or greater rights to individuals with respect to that information, than the Privacy Rule does. See the definition of "more stringent" at [45 C.F.R. 160.202](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-202.xml) for the specific criteria. For example, a State law that provides individuals with a right to inspect and obtain a copy of their medical records in a more timely manner than the Privacy Rule is "more stringent" than the Privacy Rule.

In the unusual case where a more stringent provision of State law is contrary to a provision of the Privacy Rule, the Privacy Rule provides an exception to preemption for the more stringent provision of State law, and the State law prevails. Where the more stringent State law and Privacy Rule are not contrary, covered entities must comply with both laws.

See 45 C.F.R. Part 160, Subpart B, for specific requirements related to preemption of State law. [View an unofficial version of the Privacy Rule and the preemption requirements.](https://www.hhs.gov/sites/default/files/adminsimpregtext.pdf)

# Under what circumstances will HHS grant a state law preemption exception determination?

### Answer:

The Department of Health and Human Services (HHS) may, upon specific request from a State or other entity or person, issue a determination that a contrary State law which meets certain criteria will not be preempted by the Federal requirements. Only State laws that are "contrary" to the Federal requirements are eligible for an exemption determination. As defined by HIPAA's Administrative Simplification Rules, "contrary" means that it would be impossible for a [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) to comply with both the State and Federal requirements, or that the State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. See [45 C.F.R. 160.202](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-202.xml).

A contrary State law is not preempted by the Federal requirements if the Secretary or designated HHS official determines that the request meets one or more of the following criteria, which are set forth in [45 C.F.R. 160.203](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-203.xml)(a):

1. The provision of State law is necessary
	* to prevent fraud and abuse related to the provision of or payment for health care,
	* to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation,
	* for State reporting on health care delivery and costs, or
	* for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
2. The principal purpose of the provision of State law is to regulate the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

Thus, States and other persons may request in writing that HHS except certain contrary provisions of State law from preemption by the Privacy Rule. The request for exception must explain how the State law in question is actually contrary to the Federal requirements, and how the contrary State law meets one or more of the specific criteria for which exceptions may be granted. Title 45 C.F.R. Part 160, Subpart B, sets forth the specific requirements related to preemption of State law and the criteria and process for requesting exception determinations.

HHS will not make determinations as to whether a provision of State law is "more stringent" than a provision of the HIPAA Privacy Rule, and will not determine whether a provision is "contrary" to the Privacy Rule, except in the context of, and as necessary to, making an exception determination.

# My state law provides greater privacy protections on patients’ HIV information than the HIPAA Privacy Rule. Is this more protective state law preempted by the Privacy Rule?

### Answer:

No. The Privacy Rule establishes a floor of Federal privacy protections and rights for individuals. If a provision of State law provides greater privacy protection than a provision of the Privacy Rule, and it is possible to comply with both the State law and the Privacy Rule (e.g., where a State law prohibits the disclosure of HIV status while the Privacy Rule permits such disclosure), there is no conflict between the State law and the Privacy Rule, and no preemption.

Further, even in the unusual case where a "more stringent" provision of a State law is "contrary" to a provision of the Privacy Rule – that is, it is impossible to comply with both the Privacy Rule and the State law, or the State law is an obstacle to accomplishing the full purposes and objectives of HIPAA's Administrative Simplification provisions – the Administrative Simplification Rules specifically provide an exception to preemption of State law. Thus, if a more stringent provision of State law protects HIV patient information and is contrary to the Privacy Rule, the "more stringent" State law would prevail. Because HIPAA’s Administrative Simplification Rules themselves except more stringent, contrary State law from preemption, it is neither necessary nor appropriate to request a preemption exception determination from the Department of Health and Human Services.

See [45 C.F.R. 160.202](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-202.xml) for the definitions of "more stringent" and "contrary," and [45 C.F.R. 160.203](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-203.xml) for the general rule and exceptions to preemption. [View an unofficial version of the Privacy Rule and the preemption requirements.](https://www.hhs.gov/sites/default/files/adminsimpregtext.pdf)

# My state law authorizes health care providers to report suspected child abuse to the state department of health and social services. Does the HIPAA Privacy Rule preempt this state law?

### Answer:

No. The Privacy Rule permits covered health care providers and other covered entities to disclose reports of child abuse or neglect to public health authorities or other appropriate government authorities. See [45 C.F.R. 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(b)(1)(ii). Thus, there is no conflict between the State law and the Privacy Rule, and no preemption. Covered entities may report such information and be in compliance with both the State law and the Privacy Rule.

Further, even in the unusual case where a State law that provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention is contrary to a provision of the Privacy Rule – that is, it is impossible for a covered entity to comply with both the Privacy Rule and the State law, or the State law is an obstacle to accomplishing the full purposes and objectives of HIPAA’s Administrative Simplification provisions – the Administrative Simplification Rules specifically provide an exception to preemption of State law. Thus, if a provision of State law provided for public health surveillance and was contrary to the Privacy Rule, the State law would prevail. Because the Administrative Simplification Rules except such contrary State laws from preemption, it is neither necessary nor appropriate to request a preemption exception determination from the Department of Health and Human Services.

# Will a state law preemption exception determination apply only to the entity that requested the determination?

### Answer:

No. Preemption exception determinations issued by the Department of Health and Human Services (HHS) will apply generally to all persons subject to the particular provision of State law for which the exception was granted. When an exception determination is made, HHS will promptly inform the public through publication of notice in the Federal Register, and on HHS' web sites, including the [OCR Privacy web site](https://www.hhs.gov/ocr/privacy/).

# Will HHS make determinations as to whether a provision of state law is “more stringent” than or “contrary” to a provision of the HIPAA Privacy Rule?

### Answer:

The Department of Health and Human Services (HHS) will not make determinations as to whether a provision of State law is "more stringent" than a provision of the Privacy Rule. HIPAA's Administrative Simplification Rules provide a general exception to preemption for more stringent, contrary State laws. Because such an exception already exists, it is neither necessary nor appropriate to request a preemption exception determination from HHS. Further, HHS will not determine whether a provision is "contrary" to the Privacy Rule, except in the context of, and as necessary to, making an exception determination for State laws that meet one or more of the criteria listed at [45 CFR 160.203](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-203.xml)(a).

See [45 C.F.R. 160.202](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-202.xml) for the definitions of "more stringent" and "contrary."  [View an unofficial version of the Privacy Rule and the preemption requirements.](https://www.hhs.gov/sites/default/files/adminsimpregtext.pdf)

# Will HHS publish exception determinations?

### Answer:

Yes. The Department of Health and Human Services (HHS) will promptly inform the public of exception determinations through publication of notice in the Federal Register, and on HHS' web sites, including the [OCR Privacy web site](https://www.hhs.gov/ocr/privacy/).

# What does the HIPAA Privacy Rule do?

### Answer:

Most health plans and health care providers that are covered by the new Rule must comply with the new requirements by April 14, 2003.

The HIPAA Privacy Rule for the first time creates national standards to protect individuals’ medical records and other personal health information.

* It gives patients more control over their health information.
* It sets boundaries on the use and release of health records.
* It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
* It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients’ privacy rights.
* And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

* It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
* It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
* It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
* It empowers individuals to control certain uses and disclosures of their health information.

[Learn more about health information privacy](https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html).

# Why is the HIPAA Privacy Rule needed?

### Answer:

In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. When it comes to personal information that moves across hospitals, doctors’ offices, insurers or third party payers, and State lines, our country has relied on a patchwork of Federal and State laws. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient's medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient’s permission, be passed on to a lender who could then deny the patient's application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new Federal privacy standards.

Health care providers have a strong tradition of safeguarding private health information. However, in today’s world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the Rule provides clear standards for the protection of personal health information.

# Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

### Answer:

 For the average health care provider or health plan, the Privacy Rule requires activities, such as:

* Notifying patients about their privacy rights and how their information can be used.
* Adopting and implementing privacy procedures for its practice, hospital, or plan.
* Training employees so that they understand the privacy procedures.
* Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
* Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps required by the Rule to protect patients’ privacy. [Covered entities](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) of all types and sizes are required to comply with the Privacy Rule. To ease the burden of complying with the new requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard. For example,

* The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.
* The training requirement may be satisfied by a small physician practice’s providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.
* The policies and procedures of small providers may be more limited under the Rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

# When did covered entities have to meet these HIPAA privacy standards?

### Answer:

As Congress required in HIPAA, most [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) had until April 14, 2003 to come into compliance with these standards, as modified by the August, 2002 final Rule. Small health plans had an additional year – until April 14, 2004 – to come into compliance.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is providing assistance to help covered entities prepare to comply with the Rule. Visit the [OCR Privacy web site](https://www.hhs.gov/ocr/privacy/) for helpful information, such as  guidance, frequently asked questions, sample “business associate” contract provisions, significant reference documents, and other technical assistance information for consumers and the health care industry.

# Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?

### Answer:

The consent requirement created the unintended effect of preventing health care providers from providing timely, quality health care to individuals in a variety of circumstances. The most troubling and pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to the initial face-to-face encounter with the patient, which is routinely done to provide timely access to quality health care. The following are some examples of how the consent requirement would have posed barriers to health care:

- Pharmacists would not have been able to fill a prescription, search for potential drug interactions, determine eligibility, or verify coverage before the individual arrived at the pharmacy to pick up the prescription if the individual had not already provided consent under the Privacy Rule.

- Hospitals would not have been able to use information from a referring physician to schedule and prepare for procedures before the individual presented at the hospital for such procedure, or the patient would have had to make a special trip to the hospital to sign the consent form.

- Providers who do not provide treatment in person (such as a provider prescribing over the telephone) may have been unable to provide care because they would have had difficulty obtaining prior written consent to use protected health information at the first service delivery.

- Emergency medical providers were concerned that, even if a situation was urgent, they would have had to try to obtain consent to comply with the Privacy Rule, even if that would be inconsistent with the appropriate practice of emergency medicine.

- Emergency medical providers were also concerned that the requirement that they attempt to obtain consent as soon as reasonably practicable after an emergency would have required significant efforts and administrative burden which might have been viewed as harassing by patients, because these providers typically do not have ongoing relationships with individuals.

To eliminate such barriers to health care, mandatory consent was replaced with the voluntary consent provision that permits health care providers to obtain consent for treatment, payment and healthcare operations, at their option, and enables them to obtain consent in a manner that does not disrupt needed treatment. Although consent is no longer mandatory, the Rule still affords individuals the opportunity to engage in important discussions regarding the use and disclosure of their health information through the strengthened notice requirement, while allowing activities that are essential to quality health care to occur unimpeded. These modifications will ensure that the Rule protects patient privacy as intended without harming consumers’ access to care or the quality of that care. Further, the individual’s right to request restrictions on the use or disclosure of his or her protected health information is retained in the Rule as modified.

# Will the Department of Health and Human Services (HHS) make future changes to the HIPAA Privacy Rule and, if so, how will these changes be made?

### Answer:

Under HIPAA, HHS has the authority to modify the privacy standards as the Secretary may deem appropriate. However, a standard can be modified only once in a 12-month period.

As a general rule, future modifications to the Privacy Rule must be made in accordance with the Administrative Procedure Act (APA). HHS will comply with the APA by publishing proposed rule changes, if any, in the Federal Register through a Notice of Proposed Rulemaking and will invite comment from the public. After reviewing and addressing those comments, HHS will issue a modified final rule.

# Does the HIPAA Privacy Rule create a government database with all individuals' personal health information?

### Answer:

No. The Privacy Rule does not create such a government database or require a physician or any other covered entity to send medical information to the Federal government for a government database or similar operation.

# How does the HIPAA Privacy Rule affect my rights under the Federal Privacy Act?

### Answer:

The [Privacy Act of 1974](https://www.justice.gov/opcl/privacy-act-1974) (U.S. Department of Justice) protects personal information about individuals held by the Federal government. [Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) that are Federal agencies or Federal contractors that maintain records that are covered by the Privacy Act not only must obey the Privacy Rule’s requirements, but also must comply with the Privacy Act.

# Does the HIPAA Privacy Rule protect genetic information?

### Answer:

Yes, genetic information is health information protected by the Privacy Rule. Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse. See 45 C.F.R 160.103 and 164.501.

# Does the HIPAA Privacy Rule require that covered entities document all oral communications?

### Answer:

No. The Privacy Rule does not require [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to document any information, including oral information, that is used or disclosed for treatment, payment or health care operations.

The Rule includes, however, documentation requirements for some information disclosures for other purposes. For example, some disclosures must be documented in order to meet the standard for providing a disclosure history to an individual upon request. Where a documentation requirement exists in the Rule, it applies to all relevant communications, whether in oral or some other form. For example, if a covered physician discloses information about a case of tuberculosis to a public health authority as permitted by the Rule at [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml), then he or she must maintain a record of that disclosure regardless of whether the disclosure was made orally, by phone, or in writing.

# Must a health care provider or other covered entity obtain permission from a patient prior to notifying public health authorities of the occurrence of a reportable disease?

### Answer:

No. All States have laws that require providers to report cases of specific diseases to public health officials. The HIPAA Privacy Rule permits disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. In order to do their job of protecting the health of the public, it is frequently necessary for public health officials to obtain information about the persons affected by a disease. In some cases they may need to contact those affected in order to determine the cause of the disease to allow for actions to prevent further illness.

The Privacy Rule continues to allow for the existing practice of sharing protected health information with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting deaths and births, investigating the occurrence and cause of injury and disease, and monitoring adverse outcomes related to food (including dietary supplements), drugs, biological products, and medical devices.

# Does the public health provision of the HIPAA Privacy Rule require covered entities to make public health disclosures?

### Answer:

No. The Privacy Rule’s public health provision permits, but does not require, covered entities to make such disclosures. This provision is intended to allow covered entities to continue current voluntary reporting practices that are critically important to public health and safety. The Rule also permits covered entities to disclose protected health information when State or other law requires covered entities to make disclosures for public health purposes.

For instance, many State laws require health care providers to report certain diseases, cases of child abuse, births, or deaths, and the Privacy Rule permits covered entities to disclose protected health information, without authorization, to make such reports. See the [fact sheet](https://web.archive.org/web/20080309080109/http%3A/www.hhs.gov/news/facts/privacy2007.html)about the public health provision for more information.

# May covered entities disclose facially identifiable protected health information, such as name, address, and social security number, for public health purposes?

### Answer:

Yes. The HIPAA Privacy Rule permits [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to disclose the amount and type of protected health information that is needed for public health purposes. In some cases, the disclosure will be required by other law, in which case, covered entities may make the required disclosure pursuant to [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(a) of the Rule.

For disclosures that are not required by law, covered entities may disclose, without authorization, the information that is reasonably limited to that which is minimally necessary to accomplish the intended purpose of the disclosure. For routine or recurring public health disclosures, a covered entity may develop protocols as part of its minimum necessary policies and procedures to address the type and amount of information that may be disclosed for such purposes. Covered entities may also rely on the requesting public health authority’s determination of the minimally necessary information.

# Does the HIPAA Privacy Rule's public health provision permit covered entities to disclose protected health information to authorities such as the National Institutes of Health (NIH)?

### Answer:

The definition of a “public health authority” requires that an agency’s official mandate include the responsibility for public health matters. The mandate can be responsibility for public health matters, generally, or it can be for specific public health programs. Furthermore, an agency’s official mandate does not have to be exclusively or primarily for public health. Therefore, to the extent a government agency has public health matters as part of its official mandate, it qualifies as a public health authority.

For instance, various Department of Health and Human Service (HHS) agencies, such as National Institutes of Health (NIH), and the Health Resources and Services Administration (HRSA), are authorized by law to assist the Secretary of Health and Human Services in carrying out the purposes of section 301 of the Public Health Service Act. Those agencies are public health authorities under the Rule, even if they have other non-public health mandates.

To the extent a public health authority is authorized by law to collect or receive information for the public health purposes specified in the public health provision, [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) may disclose protected health information to such public health authorities without authorization pursuant to the public health provision.

# To whom may covered entities make public health disclosures regarding a product regulated by the Food and Drug Administration (FDA) when more than one person is identified on the product label?

### Answer:

Covered entities may identify persons responsible for an FDA-regulated product by using the product label, the literature that accompanies the product, or other sources of labeling, such as the Physician’s Desk Reference. If multiple persons are named, covered entities may choose any of the persons named by these sources.

# Is a covered entity permitted to disclose protected health information under the HIPAA Privacy Rule's public health provision when the link between an averse event and a product regulated by the Food and Drug Administration (FDA) is only suspected?

### Answer:

Yes. In most instances when a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) makes an adverse event report to a person responsible for an FDA-regulated product, the covered entity will suspect, but not know, the product is the cause of the event. Determining whether the product is related to the adverse event almost always requires follow up with the covered entity which in turn may need further contact with the patient.

FDA and product manufacturers receive a great deal of important information about the safety of regulated products from these reports. To limit such reports to those instances where the covered entity is convinced of the link between the product and the event would reduce the amount of useful safety, quality and effectiveness data available to the agency as well as to product manufacturers. This would limit significantly FDA’s ability to protect the public health by helping to assure that only safe and effective products are marketed in the U.S. Accordingly, covered entities may disclose the minimum amount of protected health information that is reasonably necessary to report suspected adverse events associated with an FDA-regulated product.

# Does the HIPAA Privacy Rule's public health provision permit covered entities to disclose protected health information without authorization to a manufacturer of a product regulated by the Food and Drug Administration (FDA) for use by the manufacturer to assess the effectiveness of its marketing campaign?

### Answer:

No. The public health provision is intended to facilitate the flow of information that is essential to the FDA’s public health mission. The provision does not permit [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to disclose protected health information to a manufacturer for the manufacturer’s commercial purposes, or for any other non-public health purpose.

For example, the Rule does not permit a covered entity to provide a drug manufacturer with a list of persons who prefer a different flavored cough syrup over the flavor of the manufacturer’s product. Rather, this provision permits covered entities to disclose protected health information as necessary to continue current voluntary reporting of adverse events and similar reports that are necessary to ensure the quality, safety, or effectiveness of an FDA-regulated product.

For instance, a covered entity would be permitted to report a concern to a drug manufacturer that its cough syrup might be unsafe based on the belief that a difference in the taste could be due to drug tampering or a manufacturing problem. Likewise, a covered health care provider would be permitted to disclose protected health information to a drug manufacturer to report that the failure of a patient’s medical condition to improve may be due to the drug’s ineffectiveness. In making such a report, the covered entity may disclose the protected health information that is reasonably necessary to achieve the purpose of the report.

# Does the HIPAA Privacy Rule's public health provision permit covered health care providers to disclose protected health information concerning the findings of pre-employment physicals, drug tests, or fitness-for-duty examinations to an individuals employer?

### Answer:

The public health provision permits covered health care providers to disclose an individual's protected health information to the individual’s employer without authorization in very limited circumstances.

First, the covered health care provider must provide the health care service to the individual at the request of the individual’s employer or as a member of the employer’s workforce.

Second, the health care service provided must relate to the medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury.

Third, the employer must have a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on or act on such information. For example, OSHA requires employers to monitor employees’ exposures to certain substances and to take specific actions when an employee’s exposure level exceeds a specified limit. A [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) which tests an individual for such an exposure level at the request of the individual’s employer may disclose that test result to the employer without authorization.

Generally, pre-placement physicals, drug tests, and fitness-for-duty examinations are not performed for such purposes. However, to the extent such an examination is conducted at the request of the employer for the purpose of such workplace medical surveillance or work-related illness or injury, and the employer needs the information to comply with the requirements of OSHA, MSHA, or similar State law, the protected health information the employer needs to meet such legal obligation may be discussed to the employer without authorization. Covered health care providers who make such disclosures must provide the individual with written notice that the information is to be disclosed to his or her employer (or by posting the notice at the work site if the service is provided there).

When a health care service does not meet the above requirements, covered entities may not disclose an individual’s protected health information to the individual’s employer without an authorization, unless the disclosure is otherwise permitted without authorization by other provisions of the Rule. However, nothing in the Rule prohibits an employer from conditioning employment on an individual providing an authorization for the disclosure of such information.

# To provide individuals with an accounting for disclosures, does a covered entity have to document each medical record that may be accessed by a public health authority in the course of surveillance activities that involve all patient records?

### Answer:

The Privacy Rule does not require a notation in each medical record that has been accessed by public health authorities, as long as the information required under the Privacy Rule is included in the accounting for disclosures. Where, as with many public health disclosures, access to an entire universe of records is involved, tracking disclosures can be accomplished without the need for documentation in each record. This flexibility in the manner of documentation facilitates complying with the accounting requirement.

By way of background, a covered entity may disclose protected health information (PHI) without the patient’s authorization to a public health authority that is legally permitted to collect or receive such information for public health surveillance or related activities ([45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(b)(1)). A covered entity is also required by the Privacy Rule to account to the patient for such disclosures of PHI, if the patient asks ([45 CFR 164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml)). Further, under the Privacy Rule, making a set of records available for review by a third party constitutes a “disclosure” of the PHI in the entire set of records, regardless of whether the third party actually reviews any particular record. See [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml), for the definition of disclosure. Thus, mere access by a third party, such as a public health authority, to PHI is a disclosure and subject to an accounting for disclosures.

Public health surveillance activities often involve a retrospective review by a public health authority of a universe of patient records to identify reportable events. When a reportable case is identified, the specific data items pertinent to the public health surveillance activity are extracted and reported to the public health authority.

For example, retrospective review of the medical charts for all patients treated by a health care provider or all charts of patients treated in the entity’s emergency department may be required to identify cases of new or previously unknown infectious agents, clinical conditions associated with the use or abuse of illicit or prescription drugs, or adverse events or reactions associated with pharmaceuticals or medical devices. In these cases, as noted above, all records to which access was provided to the public health authority are deemed to have been disclosed under the Privacy Rule. Because of the universal nature of the access provided, the documentation required for the disclosure can be easily maintained. The covered entity need only document the identity (and address if known) of the public health authority to which access was provided, a description of the records and PHI subject to access, the purpose for the disclosure, and when access was provided. This documentation need not be noted in each record. It would be sufficient, for instance, for the covered entity to maintain a separate notation of such disclosures, applicable to all records so accessed. Then, if an individual requests an accounting, the covered entity need only determine whether the individual’s records were among the universe of records to which the public health authority was granted access. All individuals whose records were accessed in this fashion would receive the same accounting for the disclosure.

For example, if on August 1, 2003, a hospital began providing a public health authority ongoing access to the medical charts of all patients treated in its emergency department to identify reportable cases and extract relevant information required for a particular surveillance activity, it would be sufficient, under §164.528(b)(2), for the accounting to include the following:

* the identity, and address, if known, of the public health authority;
* a statement that the public health authority had access to medical charts for patients treated in the emergency department
* the date (or approximate range of dates) when the individual’s record was subject to access (e.g., access provided within a week of treatment in ER on [fill in date of individual visit]); and
* a statement of the purpose of the access (e.g., identify the particular public health surveillance activity).

The same basic statement could then be provided in response to a request for an accounting by any individual who was seen in the emergency department of the hospital on or after August 1, 2003.

# Can researchers continue to access existing databanks or repositories that are maintained by covered entities, even if those databases were created prior to the compliance date without patient permission or without a waiver of informed consent by an Institutional Review Board (IRB)?

### Answer

Yes. Under the HIPAA Privacy Rule, [covered entities](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) may use or disclose protected health information from existing databases or repositories for research purposes either with individual authorization as required at [45 CFR 164.508](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-508.xml), or with a waiver of individual authorization as permitted at [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(i).

# If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?

### Answer:

The Privacy Rule permits the covered entity to impose reasonable, cost-based fees. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive a summary or explanation of his or her protected health information, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information. See [45 CFR 164.524](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-524.xml).

# Does the HIPAA Privacy Rule require that covered entities provide patients with access to oral information?

### Answer:

No. The Privacy Rule requires [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to provide individuals with access to protected health information about themselves that is contained in their “designated record sets.” The term “record” in the term “designated record set” does not include oral information; rather, it connotes information that has been recorded in some manner.

The Rule does not require covered entities to tape or digitally record oral communications, nor retain digitally or tape recorded information after transcription. But if such records are maintained and used to make decisions about the individual, they may meet the definition of “designated record set.” For example, a health plan is not required to provide a member access to tapes of a telephone “advice line” interaction if the tape is maintained only for customer service review and not to make decisions about the member.

May a covered entity charge individuals a fee for providing the individuals with a copy of their PHI?

Yes, but only within specific limits. The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee to provide the individual (or the individual’s personal representative) with a copy of the individual’s PHI, or to direct the copy to a designated third party. The fee may include only the cost of certain labor, supplies, and postage:

1. Labor for copying the PHI requested by the individual, whether in paper or electronic form.  Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied.  Labor for copying does not include costs associated with reviewing the request for access; or searching for and retrieving the PHI, which includes locating and reviewing the PHI in the medical or other record, and segregating or otherwise preparing the PHI that is responsive to the request for copying.

While it has always been prohibited to pass on to an individual labor costs related to search and retrieval, our experience in administering and enforcing the HIPAA Privacy Rule has shown there is confusion about what constitutes a prohibited search and retrieval cost and this guidance further clarifies this issue.  This clarification is important to ensure that the fees charged reflect only what the Department considers “copying” for purposes of applying 45 CFR 164.524(c)(4)(i) and do not impede individuals’ ability to receive a copy of their records.
2. Supplies for creating the paper copy (e.g.,  paper, toner) or electronic media (e.g., CD or USB drive) if the  individual requests that the electronic copy be provided on portable media.  However, a covered entity may not require an  individual to purchase portable media; individuals have the right to have their  PHI e-mailed or mailed to them upon request.
3. Labor to prepare an explanation or summary of the PHI, if the individual in advance both chooses to receive an explanation or summary and agrees to the fee that may be charged.
4. Postage, when the individual requests that the copy, or the summary or explanation, be mailed.

Thus, costs associated with updates to or maintenance of systems and data, capital for data storage and maintenance, labor associated with ensuring compliance with HIPAA (and other applicable law) in fulfilling the access request (e.g., verification, ensuring only information about the correct individual is included, etc.) and other costs not included above, even if authorized by State law, are notpermitted for purposes of calculating the fees that can be charged to individuals.  See 45 CFR 164.524(c)(4).

Further, while the Privacy Rule permits the limited fee described above, covered entities should provide individuals who request access to their information with copies of their PHI free of charge.  While covered entities should forgo fees for all individuals, not charging fees for access is particularly vital in cases where the financial situation of an individual requesting access would make it difficult or impossible for the individual to afford the fee.  Providing individuals with access to their health information is a necessary component of delivering and paying for health care. We will continue to monitor whether the fees that are being charged to individuals are creating barriers to this access, will take enforcement action where necessary, and will reassess as necessary the provisions in the Privacy Rule that permit these fees to be charged.

What labor costs may a covered entity include in the fee that may be charged to individuals to provide them with a copy of their PHI?

A covered entity may include reasonable labor costs associated only with the: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; and (2) labor to prepare an explanation or summary of the PHI, if the individual in advance both chooses to receive an explanation or summary and agrees to the fee that may be charged.

Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied.  For example, labor for copying may include labor associated with the following, as necessary to copy and deliver the PHI in the form and format and manner requested or agreed to by the individual:

* Photocopying paper PHI.
* Scanning paper PHI into an electronic format.
* Converting electronic information in one format to the format requested by or agreed to by the individual.
* Transferring (e.g.,  uploading, downloading, attaching, burning) electronic PHI from a covered entity’s system to a web-based portal (where the PHI is not already maintained in or accessible through the portal), portable media, e-mail, app, personal health record, or other manner of delivery of the PHI.
* Creating and executing a mailing or e-mail with the responsive PHI.

While we allow labor costs for these limited activities, we note that as technology evolves and processes for converting and transferring files and formats become more automated, we expect labor costs to disappear or at least diminish in many cases.

In contrast, labor for copying does not include labor costs associated with:
* Reviewing the request for access.
* Searching for, retrieving, and otherwise preparing the responsive information for copying.  This includes labor to locate the appropriate designated record sets about the individual, to review the records to identify the PHI that is responsive to the request and to ensure the information relates to the correct individual, and to segregate, collect, compile, and otherwise prepare the responsive information for copying.

# May a covered health care provider charge a fee under HIPAA for individuals to access the PHI that is available through the provider’s EHR technology that has been certified as being capable of making the PHI accessible?

No. The HIPAA Privacy Rule at 45 CFR 164.524(c)(4) permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual. Where an individual requests or agrees to access her PHI available through the View, Download, and Transmit functionality of the CEHRT, we believe there are no labor costs and no costs for supplies to enable such access. Thus, a covered health care provider cannot charge an individual a fee when it fulfills an individual’s HIPAA access request using the View, Download, and Transmit functionality of the provider’s CEHRT.

# May a covered entity that uses a business associate to act on individual requests for access pass on the costs of outsourcing this function to individuals when they request copies of their PHI?

No. A covered entity may charge individuals a reasonable, cost-based fee that includes only labor for copying the PHI, costs for supplies, labor for creating a summary or explanation of the PHI if the individual requests a summary or explanation, and postage, if the PHI is to be mailed. See 45 CFR 164.524(c)(4). Administrative and other costs associated with outsourcing the function of responding to individual requests for access cannot be the basis for any fees charged to individuals for providing that access.

# Must a covered entity inform individuals in advance of any fees that may be charged when the individuals request a copy of their PHI?

Yes. When an individual requests access to her PHI and the covered entity intends to charge the individual the limited fee permitted by the HIPAA Privacy Rule for providing the individual with a copy of her PHI, the covered entity must inform the individual in advance of the approximate fee that may be charged for the copy. An individual has a right to receive a copy of her PHI in the form and format and manner requested, if readily producible in that way, or as otherwise agreed to by the individual. Since the fee a covered entity is permitted to charge will vary based on the form and format and manner of access requested or agreed to by the individual, covered entities must, at the time such details are being negotiated or arranged, inform the individual of any associated fees that may impact the form and format and manner in which the individual requests or agrees to receive a copy of her PHI. The failure to provide advance notice is an unreasonable measure that may serve as a barrier to the right of access. Thus, this requirement is necessary for the right of access to operate consistent with the HIPAA Privacy Rule.  Further, covered entities should post on their web sites or otherwise make available to individuals an approximate fee schedule for regular types of access requests.  In addition, if an individual requests, covered entities should provide the individual with a breakdown of the charges for labor, supplies, and postage, if applicable, that make up the total fee charged.  We note that this information would likely be requested in any action taken by OCR in enforcing the individual right of access, so entities will benefit from having this information readily available.

How can covered entities calculate the limited fee that can be charged to individuals to provide them with a copy of their PHI?

The HIPAA Privacy Rule permits a covered entity to charge a reasonable, cost-based fee for individuals (or their personal representatives) to receive (or direct to a third party) a copy of the individuals’ PHI. In addition to being reasonable, the fee may include only certain labor, supply, and postage costs that may apply in providing the individual with the copy in the form and format and manner requested or agreed to by the individual. The following methods may be used, as specified below, to calculate this fee.

* Actual costs. A covered entity may calculate actual labor costs to fulfill the request, as long as the labor included is only for copying (and/or creating a summary or explanation if the individual chooses to receive a summary or explanation) and the labor rates used are reasonable for such activity. The covered entity may add to the actual labor costs any applicable supply (e.g., paper, or CD or USB drive) or postage costs. Covered entities that charge individuals actual costs based on each individual access request still must be prepared to inform individuals in advance of the approximate fee that may be charged for providing the individual with a copy of her PHI. An example of an actual labor cost calculation would be to time how long it takes for the workforce member of the covered entity (or business associate) to make and send the copy in the form and format and manner requested or agreed to by the individual and multiply the time by the reasonable hourly rate of the person copying and sending the PHI. What is reasonable for purposes of an hourly rate will vary depending on the level of skill needed to create and transmit the copy in the manner requested or agreed to by the individual (e.g., administrative level labor to make and mail a paper copy versus more technical skill needed to convert and transmit the PHI in a particular electronic format).
* Average costs. In lieu of calculating labor costs individually for each request, a covered entity can develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, as long as the types of labor costs included are the ones which the Privacy Rule permits to be included in a fee (e.g., labor costs for copying but not for search and retrieval) and are reasonable. Covered entities may add to that amount any applicable supply (e.g., paper, or CD or USB drive) or postage costs.
	+ This standard rate can be calculated and charged as a per page fee only in cases where the PHI requested is maintained in paper form and the individual requests a paper copy of the PHI or asks that the paper PHI be scanned into an electronic format. Per page fees are notpermitted for paper or electronic copies of PHI maintained electronically. OCR is aware that per page fees in many cases have become a proxy for fees charged for all types of access requests – whether electronic or paper – and that many states with authorized fee structures have not updated their laws to account for efficiencies that exist when generating copies of information maintained electronically. This practice has resulted in fees being charged to individuals for copies of their PHI that do not appropriately reflect the permitted labor costs associated with generating copies from information maintained in electronic form. Therefore, OCR does not consider per page fees for copies of PHI maintained electronically to be reasonable for purposes of 45 CFR 164.524(c)(4).
* Flat fee for electronic copies of PHI maintained electronically. A covered entity may charge individuals a flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage. Charging a flat fee not to exceed $6.50 is therefore an option for entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically.

# Is $6.50 the maximum amount that can be charged to provide individuals with a copy of their PHI?

No. For any request from an individual, a covered entity (or business associate operating on its behalf) may calculate the allowable fees for providing individuals with copies of their PHI: (1) by calculating actual allowable costs to fulfill each request; or (2) by using a schedule of costs based on average allowable labor costs to fulfill standard requests. Alternatively, in the case of requests for an electronic copy of PHI maintained electronically, covered entities may: (3) charge a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and postage). Charging a flat fee not to exceed $6.50 per request is therefore an option available to entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically.

In some cases where an entity chooses generally to use the average cost method, or chooses a flat fee, as described above, for electronic copies of PHI maintained electronically, the entity may receive an unusual or uncommon type of request that it had not considered in setting up its fee structure. In these cases, the entity may wish to calculate actual costs to provide the requested copy, and it may do so as long as the costs are reasonable and only of the type permitted by the Privacy Rule. An entity that chooses to calculate actual costs in these circumstances still must—as in other cases—inform the individual in advance of the approximate fee that may be charged for providing the copy requested.

# Are costs authorized by State fee schedules permitted to be charged to individuals when providing them with a copy of their PHI under the HIPAA Privacy Rule?

No, except in cases where the State authorized costs are the same types of costs permitted under 45 CFR 164.524(c)(4) of the HIPAA Privacy Rule, and are reasonable. The bottom line is that the costs authorized by the State must be those that are permitted by the HIPAA Privacy Rule and must be reasonable. The HIPAA Privacy Rule at 45 CFR 164.524(c)(4) permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual. Thus, labor (e.g., for search and retrieval) or other costs not permitted by the Privacy Rule may not be charged to individuals even if authorized by State law. Further, a covered entity’s fee for providing an individual with a copy of her PHI must be reasonable in addition to cost-based, and there may be circumstances where a State authorized fee is not reasonable, even if the State authorized fee covers only permitted labor, supply, and postage costs. For example, a State-authorized fee may be higher than the covered entity’s cost to provide the copy of PHI. In addition, many States with authorized fee structures have not updated their laws to account for efficiencies that exist when generating copies of information maintained electronically. Therefore, these State authorized fees for copies of PHI maintained electronically may not be reasonable for purposes of 45 CFR 164.524(c)(4)

# A State law requires that a health care provider give individuals one free copy of their medical records but HIPAA permits the provider to charge a fee. Does HIPAA override the State law?

No, so the health care provider must comply with the State law and provide the one free copy. In contrast to State laws that authorize higher or different fees than are permitted under HIPAA, HIPAA does not override those State laws that provide individuals with greater rights of access to their health information than the HIPAA Privacy Rule does. See 45 CFR 160.202 and 160.203. This includes State laws that: (1) prohibit fees to be charged to provide individuals with copies of their PHI; or (2) allow only lesser fees than what the Privacy Rule would allow to be charged for copies.

# When do the HIPAA Privacy Rule limitations on fees that can be charged for individuals to access copies of their PHI apply to disclosures of the individual’s PHI to a third party?

The fee limits apply when an individual directs a covered entity to send the PHI to the third party.  Under the HIPAA Privacy Rule, a covered entity is prohibited from charging an individual who has requested a copy of her PHI more than a reasonable, cost-based fee for the copy that covers onlycertain labor, supply, and postage costs that may apply in fulfilling the request.  See 45 CFR 164.524(c)(4).  This limitation applies regardless of whether the individual has requested that the copy of PHI be sent to herself, or has directed that the covered entity send the copy directly to a third party designated by the individual (and it doesn’t matter who the third party is).  To direct a copy to a third party, the individual’s access request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI.  See 45 CFR 164.524(c)(3)(ii).  Thus, written access requests by individuals to have a copy of their PHI sent to a third party that include these minimal elements are subject to the same fee limitations in the Privacy Rule that apply to requests by individuals to have a copy of their PHI sent to themselves.  This is true regardless of whether the access request was submitted to the covered entity by the individual directly or forwarded to the covered entity by a third party on behalf and at the direction of the individual (such as by an app being used by the individual).  Further, these same limitations apply when the individual’s personal representative, rather than the individual herself, has made the request to send a copy of the individual’s PHI to a third party.

In contrast, third parties often will directly request PHI from a covered entity and submit a written HIPAA authorization from the individual (or rely on another permission in the Privacy Rule) for that disclosure.  Where the third party is initiating a request for PHI on its own behalf, with the individual’s HIPAA authorization (or pursuant to another permissible disclosure provision in the Privacy Rule), the access fee limitations do not apply.  However, as described above, where the third party is forwarding - on behalf and at the direction of the individual - the individual’s access request for a covered entity to direct a copy of the individual’s PHI to the third party, the fee limitations apply.

We note that a covered entity (or a business associate) may not circumvent the access fee limitations by treating individual requests for access like other HIPAA disclosures – such as by having an individual fill out a HIPAA authorization when the individual requests access to her PHI (including to direct a copy of the PHI to a third party).  As explained elsewhere in the guidance, a HIPAA authorization is not required for individuals to request access to their PHI, including to direct a copy to a third party – and because a HIPAA authorization requests more information than is necessary or that may not be relevant for individuals to exercise their access rights, requiring execution of a HIPAA authorization may create impermissible obstacles to the exercise of this right.  Where it is unclear to a covered entity, based on the form of a request sent by a third party, whether the request is an access request initiated by the individual or merely a HIPAA authorization by the individual to disclose PHI to the third party, the entity may clarify with the individual whether the request was a direction from the individual or a request from the third party.  OCR is open to engaging with the community on ways that technology could easily convey this information.

Finally, we note that disclosures to a third party made outside of the right of access under other provisions of the Privacy Rule still may be subject to the prohibition against sales of PHI (i.e., the prohibition against receiving remuneration for a disclosure of PHI at 45 CFR 164.502(a)(5)(ii)).  Where the prohibition applies, a covered entity may charge only a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by other law or must have received a HIPAA authorization from the individual that states that the disclosure will involve remuneration to the covered entity.

# May a health care provider withhold a copy of an individual’s PHI from the individual who requested it because the covered entity used the individual’s payment of the allowable fee for the copy to instead pay an outstanding bill for health care services provided to the individual?

No. Just as a covered entity may not withhold or deny an individual access to his PHI on the grounds that the individual has not paid the bill for health care services the covered entity provided to the individual, a covered entity may not withhold or deny access on the grounds that the covered entity used the individual’s payment of the fee for a copy of his PHI to offset or pay the individual’s outstanding bill for health care services.

# Can an individual be charged a fee if the individual requests only to inspect her PHI at the covered entity (i.e., does not request that the covered entity produce a copy of the PHI)?

No. The fees that can be charged to individuals exercising their right of access to their PHI apply only in cases where the individual is to receive a copy of the PHI, versus merely being provided the opportunity to view and inspect the PHI. The HIPAA Privacy Rule provides individuals with the right to inspect their PHI held in a designated record set, either in addition to obtaining copies or in lieu thereof, and requires covered entities to arrange with the individual for a convenient time and place to inspect the PHI. See 45 CFR 164.524(c)(1) and (c)(2). Consequently, covered entities should have in place reasonable procedures to enable individuals to inspect their PHI, and requests for inspection should trigger minimal additional effort by the entity, particularly where the PHI requested is of the type easily accessed onsite by the entity itself in the ordinary course of business. For example, covered entities could use the capabilities of Certified EHR Technology (CEHRT) to enable individuals to inspect their PHI, if the individuals agree to the use of this functionality.

Further, a covered entity may not charge an individual who, while inspecting her PHI, takes notes, uses a smart phone or other device to take pictures of the PHI, or uses other personal resources to capture the information. If the individual is making the copies of PHI using her own resources, the covered entity may not charge a fee for those copies, as the copying is being done by the individual and not the entity. A covered entity may establish reasonable policies and safeguards regarding an individual’s use of her own camera or other device for copying PHI to assure that equipment or technology used by the individual is not disruptive to the entity’s operations and is used in a way that enables the individual to copy or otherwise memorialize only the records to which she is entitled. Further, a covered entity is not required to allow the individual to connect a personal device to the covered entity’s systems.

Can an individual, through the HIPAA right of access, have his or her health care provider or health plan send the individual’s PHI to a third party?

Yes. If requested by an individual, a covered entity must transmit an individual’s PHI directly to another person or entity designated by the individual. The individual’s request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI. See 45 CFR 164.524(c)(3)(ii). A covered entity may accept an electronic copy of a signed request (e.g., PDF or scanned image), an electronically executed request (e.g., via a secure web portal) that includes an electronic signature, or a faxed or mailed copy of a signed request.

The same requirements for providing the PHI to the individual, such as the timeliness requirements, fee limitations, prohibition on imposing unreasonable measures, and form and format requirements, apply when an individual directs that the PHI be sent to another person or entity. For example, just as when the individual requests a copy for herself, a covered entity cannot require that an individual make a separate in person trip to the covered entity’s physical location for the purpose of making the request to transmit the individual’s PHI to a person or entity designated by the individual. In addition, the individual can designate the form and format of the PHI and how the PHI is to be sent to the third party, and the covered entity must provide access in the requested form and format and manner if the PHI is “readily producible” in such a way. Whether PHI is “readily producible” depends on the capabilities of the covered entity and whether transmission or transfer of the PHI in the requested manner would present an unacceptable level of security risk to the PHI on the covered entity’s systems (based on the covered entity’s Security Rule risk analysis).

The following are just a few examples of how these provisions apply:

* A patient requests in writing that the hospital where she recently underwent a surgical procedure use its Certified EHR Technology (CEHRT) to send her discharge summary to her primary care physician, or to her own personal health record, and she supplies the corresponding Direct address (an electronic address for securely exchanging health information using the Direct technical standard).
* A patient sends a written request to his long-time physician asking the physician to download a copy of the PHI from his electronic medical record, and e-mail it in encrypted form to XYZ Research Institution, at XYZResearch@anywhere.com, so XYZ Research Institution can use his health information for research purposes.
* A patient requests in writing that her ob-gyn digitally transmit records of her latest pre-natal visit to a new pregnancy self-care app that she has on her mobile phone. The ob-gyn’s EHR has the ready capability to establish the connection in a manner that does not present an unacceptable level of security risk to the PHI in the EHR or other of the ob-gyn’s systems, based on the ob-gyn’s Security Rule risk analysis.

In each of these three examples, the covered entity has the capability to transfer the PHI in the requested manner and doing so would not present an unacceptable level of security risk to the PHI in the covered entity’s systems. Thus, after receiving the patient’s written request, the covered entity has 30 days (or 60 days if an extension is applicable) to send the PHI to the designated recipient as directed by the individual. However, in most cases, it is expected that the use of technology will enable the covered entity to fulfill the individual’s request in far fewer than 30 days.

Are there any limits or exceptions to the individual’s right to have the individual’s PHI sent directly to a third party?

The right of an individual to have PHI sent directly to a third party is an extension of the individual’s right of access; consequently, all of the provisions that apply when an individual obtains access to her PHI apply when she directs a covered entity to send the PHI to a third party. As a result:

* This right applies to PHI in a designated record set;
* Covered entities must take action within 30 days of the request;
* Covered entities must provide the PHI in the form and format and manner of access requested by the individual if it is “readily producible” in that manner; and
* The individual may be charged only a reasonable, cost-based fee that complies with 45 CFR 164.524(c)(4).

Further, the same limited grounds for denial of access that apply when the individual is receiving the PHI directly apply in cases where the individual requests that the PHI be provided to a designated third party. See 45 CFR 164.524(a)(2) and (a)(3). Thus, for example, a covered entity may deny an individual’s request to send PHI to a designated third party when the request is for psychotherapy notes or PHI for which a licensed health care professional has determined, exercising professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. The provisions of the Privacy Rule providing for review of certain denials of access apply in this circumstance as well. See 45 CFR 164.524(a)(3) and (a)(4). However, a covered entity may not deny an individual’s access request to send PHI to a third party for other purposes. Thus, disagreement with the individual about the worthiness of the third party as a recipient of PHI, or even concerns about what the third party might do with the PHI (except for the express reasons listed in the Privacy Rule, such as in cases where life or physical safety is threatened), are not acceptable reasons to deny an individual’s request.

# Can an individual’s personal representative, through the HIPAA right of access, have the individual’s health care provider or health plan send the individual’s PHI to a third party?

Yes. An individual’s personal representative (generally, a person with authority under State law to make health care decisions for the individual) has the right both to receive a copy of PHI about the individual in a designated record set, and to direct the covered entity to transmit a copy of the PHI to another person or entity, upon request, consistent with the scope of such representation and the requirements of 45 CFR 164.524. See 45 CFR 164.502(g). The same requirements for fulfilling an individual’s request to send the individual’s PHI to a third party (e.g., with respect to timeliness, form and format, bases for denial, fee limitations, etc.) also apply to requests made by an individual’s personal representative.

# What is the liability of a covered entity in responding to an individual’s access request to send the individual’s PHI to a third party?

Covered entities may rely on the information provided in writing by the individual about the identity of the designated person and where to send the PHI for purposes of verification of the designated third party as an authorized recipient. However, covered entities must implement reasonable safeguards in otherwise carrying out the request, such as taking reasonable steps to verify the identity of the individual making the access request and to enter the correct information into the covered entity’s system. For example, while a covered entity is not required to confirm that the individual provided the correct e-mail address of the third party, the covered entity is required to have reasonable procedures to ensure that it correctly enters the provided e-mail address into the covered entity’s system.

In addition, except in the limited circumstance described below, covered entities must safeguard the information in transit, and are responsible for breach notification and may be liable for impermissible disclosures of PHI that occur in transit. The only exception arises when an individual has requested that the PHI be sent to the third party by unencrypted e-mail or in another unsecure manner, which the individual has a right to request. As long as the individual was warned of and accepted the security risks to the PHI associated with the unsecure transmission, the covered entity is not responsible for breach notification or liable for disclosures that occur in transit.

Further, the covered entity is not liable for what happens to the PHI once the designated third party receives the information as directed by the individual in the access request.

# What is a covered entity’s obligation under the Breach Notification Rule if it transmits an individual’s PHI to a third party designated by the individual in an access request, and the entity discovers the information was breached in transit?

If a covered entity discovers that the PHI was breached in transit to the designated third party, and the PHI was “unsecured PHI” as defined at 45 CFR 164.402, the covered entity generally is obligated to notify the individual and HHS of the breach and otherwise comply with the HIPAA Breach Notification Rule at 45 CFR 164, Subpart D. However, if the individual requested that the covered entity transmit the PHI in an unsecure manner (e.g., unencrypted), and, after being warned of the security risks to the PHI associated with the unsecure transmission, maintained her preference to have the PHI sent in that manner, the covered entity is not responsible for a disclosure of PHI while in transmission to the designated third party, including any breach notification obligations that would otherwise be required. Further, a covered entity is not liable for what happens to the PHI once the designated third party receives the information as directed by the individual in the access request.

Where the PHI that was breached is “secured” as provided for in the HHS Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (available at [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html](https://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html)), the covered entity does not have reporting obligations under the Breach Notification Rule.

# Why depend on the individual’s right of access to facilitate the disclosure of PHI to a third party – why not just have the individual execute a HIPAA authorization to enable the covered entity to make this disclosure?

The PHI that an individual wants to have disclosed to a third party under the HIPAA right of access also could be disclosed by a covered entity pursuant to a valid HIPAA authorization.  However, there are differences between the two methods – the primary difference being that one is a required disclosure and one is a permitted disclosure -- that may make the right of access a more favorable choice for most disclosures the individual is initiating on her own behalf.  These differences are illustrated in the following table:

|  |  |
| --- | --- |
| **HIPAA Authorization** | **Right of Access** |
| **Permits**, but does not require, a covered entity to disclose PHI | **Requires** a covered entity to disclose PHI, except where an exception applies |
| Requires a number of elements and statements, which include a description of who is authorized to make the disclosure and receive the PHI, a specific and meaningful description of the PHI, a description of the purpose of the disclosure, an expiration date or event, signature of the individual authorizing the use or disclosure of her own PHI and the date, information concerning the individual’s right to revoke the authorization, and information about the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization. | Must be in writing, signed by the individual, and clearly identify the designated person and where to the send the PHI |
| No timeliness requirement for disclosing the PHI Reasonable safeguards apply (e.g., PHI must be sent securely) | Covered entity must act on request no later than 30 days after the request is received |
| Reasonable safeguards apply (e.g., PHI must be sent securely) | Reasonable safeguards apply, including a requirement to send securely; however, individual can request transmission by unsecure medium  |
| No limitations on fees that may be charged to the person requesting the PHI; however, if the disclosure constitutes a sale of PHI, the authorization must disclose the fact of remuneration  | Fees limited as provided in 45 CFR 164.524(c)(4)  |

In addition, the Privacy Rule permits covered entities to disclose PHI for treatment, payment and health care operations without the need to first obtain an individual’s authorization or receive an access request by the individual to have the individual’s PHI directed to a third party for such purposes. See 45 CFR 164.506. As a result, if an individual is seeking to have her PHI shared among her treating providers, the covered entities can and should do so; the individual should not have to facilitate this transmission by submitting an access request (and potentially having to wait up to 30 days for the information to be sent and be charged a fee) or by executing a HIPAA authorization. See the Fact Sheets on Understanding Some of HIPAA’s Permitted Uses and Disclosures at [http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/permitted-uses/index.html](http://hhs.gov/hipaa/for-professionals/privacy/guidance/permitted-uses/index.html).

# What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans?

With limited exceptions, the HIPAA Privacy Rule gives individuals the right to access, upon request, the medical and health information (protected health information or PHI) about them in one or more designated record sets maintained by or for the individuals’ health care providers and health plans (HIPAA covered entities). See 45 CFR 164.524. Designated record sets include medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals. See 45 CFR 164.501. Thus, individuals have a right to access a broad array of health information about themselves, whether maintained by a covered entity or by a business associate on the covered entity’s behalf, including medical records, billing and payment records, insurance information, clinical laboratory test reports, X-rays, wellness and disease management program information, and notes (such as clinical case notes or “SOAP” notes (a method of making notes in a patient’s chart) but not including psychotherapy notes as explained below), among other information generated from treating the individual or paying for the individual’s care or otherwise used to make decisions about individuals. In responding to a request for access, a covered entity is not, however, required to create new information, such as explanatory materials or analyses, that does not already exist in the designated record set. Further, while individuals have a right to a broad array of PHI about themselves in a designated record set, a covered entity is only required to provide access to the PHI to which the individual requests access.

Individuals do not have a right to access PHI about them that is not part of a designated record set because this information is not used to make decisions about individuals. This may include certain quality assessment or improvement records, patient safety activity records, or business planning, development, and management records that are used for business decisions more generally rather than to make decisions about individuals. For example, peer review files, practitioner or provider performance evaluations, quality control records used to improve customer service, and formulary development records may be generated from and include an individual’s PHI but may not be in the covered entity’s designated record set(s) to which the individual has access. However, the underlying PHI from the individual’s medical or payment records used to generate such information remains part of the designated record set and subject to access by the individual. For example, an individual would not have the right to access internal memos related to the development of a formulary; however, an individual does have the right to access information about prescription drugs that were prescribed for her, and claims records related to payment for those drugs, even if that information was relied on in, or helped inform, the development of the formulary.

Individuals also do not have a right to access the psychotherapy notes that a mental health professional maintains separately from the individual’s medical record and that document or analyze the contents of a counseling session with the individual. In addition, individuals do not have a right to access information about the individual compiled in reasonable anticipation of, or for use in, a legal proceeding (but the individual retains the right to access the underlying PHI from the designated record set(s) about the individual used to generate the litigation information). However, a covered entity has the discretion to share this information with the individual if it chooses. See 45 CFR 164.524(a)(1) – (a)(3) for a complete list of exceptions to the right of access.

# Does an individual’s right under HIPAA to access their health information apply only to the information a health care provider maintains about the individual in an Electronic Health Record (EHR), or paper medical record?

No. An individual has a broad right under the HIPAA Privacy Rule to access the PHI about the individual in all designated record sets maintained by or for a covered entity, whether in electronic or paper form, not just the designated record set that comprises the “medical record.” See 45 CFR 164.524(a). (However, if the same PHI is maintained in more than one designated record set, a covered entity need only produce the information once in response to a request for access.) A designated record set also includes billing and payment records, claims and insurance information, as well as other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals. See the definition of “designated record set” at 45 CFR 164.501.

# Does the individual have a right to access PHI about themselves maintained by a covered entity that is very old or is archived?

Yes. An individual has a right to access PHI about themselves in a medical record or other designated record set maintained by a covered entity, regardless of the date the information was created or whether the information is maintained onsite, remotely, or is archived. There are only very limited grounds under which a covered entity may deny an individual access to PHI about herself in a designated record set, which do not include the age or location of the information. See 45 CFR 164.524(a)(2) – (a)(3).

# Does an individual have a right to access all of the information a covered entity maintains in the individual’s medical record?

Yes. Except in very limited circumstances, an individual has a right to access all PHI about the individual that a covered entity (or its business associate) maintains in one or more designated record sets. A designated record set is defined to include the medical record about the individual. Thus, an individual generally has a right to access all of the information about the individual that a covered entity maintains in the individual’s medical record, including information the individual provided to the covered entity herself, as well as PHI about the individual contributed to the record by other health care providers or covered entities. See 45 CFR 164.524(a)(2) – (a)(3) for the limited grounds upon which a covered entity may deny an individual access to PHI in a designated record set.

# Under what circumstances may a covered entity deny an individual’s request for access to the individual’s PHI?

A covered entity may deny an individual access to all or a portion of the PHI requested in only very limited circumstances. For example, a covered entity may deny an individual access if the information requested is not part of a designated record set maintained by the covered entity (or by a business associate for a covered entity), or the information is excepted from the right of access because it is psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a legal proceeding (but the individual retains the right to access the underlying PHI from the designated record set(s) about the individual used to generate this information).

Another limited ground for denial exists if a licensed health care professional determines in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. For example, a covered entity may deny a suicidal patient access to information that a provider determines in his professional judgment is reasonably likely to lead the patient to take her own life. However, we stress that this ground is narrowly construed in order to protect individuals’ autonomy interests and their right under the Privacy Rule to obtain information about themselves, which is fundamental in facilitating individuals’ active participation in their own health care. General concerns about psychological or emotional harm are not sufficient to deny an individual access (e.g., concerns that the individual will not be able to understand the information or may be upset by it). In addition, the requested access must be reasonably likely to cause harm or endanger physical life or safety. Thus, concerns based on the mere possibility of harm are not sufficient to deny access. As a result, we expect this ground for denial to apply in extremely rare circumstances. Further, an individual who is denied access based on these grounds has a right to have the denial reviewed by a licensed health care professional designated by the covered entity as a reviewing official who did not participate in the original decision to deny access.

For a complete list of the grounds and conditions for denial of access, see 45 CFR 164.524(a)(2)-(4). Note that an individual may not be required to provide a reason for requesting access, and the individual’s rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is not a permitted reason to deny access.

If a covered entity denies access, in whole or in part, to PHI requested by the individual based on one or more permitted grounds, the covered entity must provide a denial in writing to the individual no later than 30 calendar days after the request (or no more than 60 calendar days if the covered entity notified the individual of an extension). See 45 CFR 164.524(b)(2). The denial must be in plain language and describe the basis for denial; if applicable, the individual’s right to have the decision reviewed and how to request such a review; and how the individual may submit a complaint to the covered entity or the HHS Office for Civil Rights. See 45 CFR 164.524(d).

The covered entity must, to the extent possible, provide the individual with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access. See 45 CFR 164.524(d)(1).

# Does an individual have a right under HIPAA to access PHI about the individual maintained by a business associate of a covered entity?

Yes. An individual’s right under the HIPAA Privacy Rule to access PHI about themselves extends to PHI in a designated record set maintained by a business associate on behalf of a covered entity. Thus, if an individual submits a request for access to PHI, the covered entity is responsible for providing the individual with access not only to the PHI it holds but also to the PHI held by one or more of its business associates. However, if the same PHI that is the subject of an access request is maintained in both the designated record set of the covered entity and the designated record set of the business associate, the PHI need only be produced once in response to the request for access. See 45 CFR 164.524(c)(1).

With respect to PHI in a designated record set maintained by a business associate, the business associate agreement between the covered entity and the business associate will govern whether the business associate will provide access directly to the individual or will provide the PHI that is the subject of the individual’s access request to the covered entity for the covered entity to then provide access to the individual. However, regardless of how and to what extent a business associate supports or fulfills a covered entity’s obligation to provide access to an individual, a request for access still must be acted upon within 30 calendar days (or 60 calendar days if an extension is applicable) of receipt of the request by either the covered entity, or by a business associate if the request was made directly to the business associate because the covered entity instructed individuals through its notice of privacy practices (or otherwise) to submit access requests directly to the business associate. Further, all of the access requirements that apply with respect to PHI held by the covered entity (e.g., limitations on fees that may be charged) apply with respect to PHI held by the business associate.

# Does an individual have a right under HIPAA to access from a clinical laboratory the genomic information the laboratory has generated about the individual?

Yes. An individual has a right under the HIPAA Privacy Rule to access, upon request, PHI about the individual in a designated record set maintained by or for a clinical laboratory that is a covered entity. The designated record set includes not only the laboratory test reports but also the underlying information generated as part of the test, as well as other information concerning tests a laboratory runs on an individual. For example, a clinical laboratory that is a HIPAA covered entity and that conducts next generation sequencing (NGS) of DNA on an individual must provide the individual, upon the individual’s request for PHI concerning the NGS, with a copy of the completed test report, the full gene variant information generated by the test, as well as any other information in the designated record set concerning the test.

# Does an individual have a right under HIPAA to access more than just test results from a clinical laboratory?

Yes. Under the HIPAA Privacy Rule, an individual has a general right to access, upon request, PHI about the individual in a designated record set maintained by or for a clinical laboratory that is a covered entity. A test result or test report is only part of the designated record set a clinical laboratory may hold. To the extent an individual requests access to all of her information held by the laboratory, the laboratory is required to provide access to all of the PHI about the individual in its designated record set. This could include, for example, completed test reports and the underlying data used to generate the reports, test orders, ordering provider information, billing information, and insurance information.

How timely must a covered entity be in responding to individuals’ requests for access to their PHI?

Under the HIPAA Privacy Rule, a covered entity must act on an individual’s request for access no later than 30 calendar days after receipt of the request. If the covered entity is not able to act within this timeframe, the entity may have up to an additional 30 calendar days, as long as it provides the individual – within that initial 30-day period – with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request. See 45 CFR 164.524(b)(2).

These timelines apply regardless of whether:

* The PHI that is the subject of the request is maintained by the covered entity or by a business associate on behalf of the covered entity, or the covered entity uses a business associate to fulfill individual requests for access. The 30-day clock starts on the date that the covered entity receives a request for access, so any delay in obtaining the necessary information from a business associate or forwarding the request to the business associate for action “uses up” part of the allotted time. Alternatively, the 30-day clock starts when, instead of the covered entity, a business associate receives a request directly from an individual because the covered entity instructed the individual through its notice of privacy practices (or otherwise) to submit the access request directly to its business associate for processing.
* The covered entity negotiates with the individual on the format of the response. Covered entities that spend significant time before reaching agreement with individuals on format are depleting the 30 days allotted for the response by that amount of time.
* The PHI that is the subject of the request is old, archived, and/or not otherwise readily accessible.

These timelines are outer limits, and it is expected that many covered entities should be able to respond to requests for access well before these outer limits are reached. However, in cases where a covered entity is aware that an access request may take close to these outer time limits to fulfill, the entity is encouraged to provide the requested information in pieces as it becomes available, if the individual indicates a desire to receive the information in such a manner.

# Under the EHR Incentive Program, participating providers are required to provide individuals with access to certain information on much faster timeframes (e.g., a discharge summary within 36 hours of discharge, a lab result within 4 business days after the provider has received the results) than under HIPAA. How do these requirements operate together?

Health care providers participating in the EHR Incentive Program may use the patient engagement tools of their Certified EHR Technology to make certain information available to patients quickly and satisfy their EHR Incentive Program objectives. Doing so also has the added benefit of satisfying an individual’s request for access under HIPAA, where the PHI requested by the individual is available through the Certified EHR Technology, and the individual agrees to access the information in this way. While the Privacy Rule permits a covered entity to take up to 30 calendar days from receipt of a request to provide access (with one extension for up to an additional 30 calendar days when necessary), covered entities are strongly encouraged to provide individuals with access to their health information much sooner, and to take advantage of technologies that enable individuals to have faster or even immediate access to the information.

# Why does HIPAA give covered entities 30 days to respond to individuals’ requests for access to their PHI? In the digital age, allowing covered entities 30 days to provide individuals with access to their health information seems too long; individuals need this information promptly to manage their health and health care.

While some individual access requests should be fairly easy to fulfill (e.g., those that can be satisfied through the use of Certified EHR Technology), the HIPAA Privacy Rule recognizes that there may be other circumstances where additional time and effort may be necessary to locate and obtain the PHI that is the subject of the request, or to provide the PHI in the format requested or agreed to by the individual, or otherwise to act on the request. The Privacy Rule is intended to set the outer time limit for providing access, not indicate the desired or best result, and it is expected that many covered entities should be able to respond to requests for access well before the 30 day outer limit. Further, as technology evolves and PHI becomes more readily available via easy-to-use digital technologies, the ability to provide very prompt or almost instantaneous access to individuals will increase. The Department will continue to monitor these developments.

# In some cases, the 30-day timeframe from a request to provide an individual with access to her PHI may not be sufficient time for a clinical laboratory to complete the test report that is the subject of the individual’s request. What can a clinical laboratory do in these cases?

In those limited cases where, due to the nature of the test and the timing of the individual’s request, 30 calendar days may not be sufficient to complete a test report to which the individual has requested access, the laboratory may notify the individual in writing within the 30-day period of the need and specific reason for the delay in providing access to the completed test result and the date by which the laboratory will complete its action on the request, in accordance with § 164.524(b)(2)(iii) of the HIPAA Privacy Rule. The Privacy Rule allows only one extension on an access request and the extension may not exceed an additional 30 calendar days. In the rare circumstance where 60 calendar days is not sufficient to provide the individual with access to the completed test report requested by the individual, the covered laboratory may, at the end of the 60 day period, satisfy the access request by providing the individual with access to the PHI that does exist at the time (e.g., test requisitions, the underlying data being used to generate the reports, other completed test reports) in the designated record set.

However, to avoid this situation to the extent possible, in cases where the laboratory knows that a particular test report will take longer than the HIPAA access timeframes, we expect the laboratory to explain this circumstance to the individual. Upon informing individuals of this situation when they request access, the individuals may be willing to withdraw or hold their request until a later time to ensure that they get access to what they want or need. If an individual chooses not to withdraw his or her request for access, the individual will then have a right only to obtain the PHI in the designated record set at the time the request is fulfilled, which may not include the particular test report requested because it is not yet complete.

# Under the HIPAA Privacy Rule, do individuals have the right to an electronic copy of their PHI?

Yes, in most cases. If the PHI is maintained by a covered entity electronically, an individual has a right to receive an electronic copy of the information upon request (assuming the covered entity does not have a ground for denial under 45 CFR 164.524(a)(2) or (a)(3)). The covered entity must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in that form and format, or if not, in a readable alternative electronic format as agreed to by the individual and covered entity. See 45 CFR 164.524(c)(2)(ii). Where an individual requests access to PHI that is maintained electronically by a covered entity, the covered entity may provide the individual with a paper copy of the PHI to satisfy the request only in cases where the individual declines to accept any of the electronic formats readily producible by the covered entity.

If the individual requests an electronic copy of PHI that the covered entity maintains only on paper, the covered entity must provide the individual with the electronic copy if the copy is readily producible electronically (e.g., the covered entity can readily scan the paper record into an electronic format) and in the electronic format requested if readily producible in that format, or if not, in a readable alternative electronic format as agreed to by the covered entity and individual. If the copy is not readily producible in electronic form, or the individual declines to accept the electronic format(s) readily producible by the covered entity, then a readable hard copy of the PHI may be provided to satisfy the access request. See 45 CFR 164.524(c)(2)(i).

# If an individual requests an electronic copy of the individual’s PHI that the covered entity maintains only on paper, is the covered entity required to scan the paper records to create an electronic copy of the PHI for the individual?

While a covered entity is not required to purchase a scanner to create electronic copies, if a covered entity can readily produce an electronic copy of the PHI for the individual by scanning the records, it must do so. In particular, if an individual requests an electronic copy of PHI in a specific format, and a covered entity maintains that PHI only on paper, the covered entity must provide the individual with the electronic copy, in the format requested, if the copy is readily producible electronically and readily producible in the electronic format requested. If the copy is readily producible electronically but not in the specific format requested, the covered entity may offer the individual the copy in an alternative readable electronic format. If the copy is not readily producible in electronic form, or the individual declines to accept the electronic format(s) that are readily producible by the covered entity, then the covered entity may provide the individual with a readable hard copy of the PHI to satisfy the access request. See § 164.524(c)(2)(i). For example, a covered entity that maintains the requested PHI only on paper may be able to readily produce a scanned PDF version of the PHI but not the requested Word version. In this case, the covered entity may provide the individual with the PDF version if the individual agrees to accept the PDF version. If the individual declines to accept the PDF version, or if the covered entity is not able to readily produce a PDF or other electronic version of the PHI, the covered entity may provide the individual with a hard copy, such as a photocopy, of the PHI.

# When an individual exercises her HIPAA right to get an electronic copy of her PHI, can the individual choose the electronic format of the copy?

While individuals do not have an unlimited choice in the form of electronic copy requested, and covered entities are not required to purchase new software or other equipment in order to accommodate every possible individual request, the individual does have a right to receive the copy in the form and format requested by the individual if the copy is readily producible in that form and format. For example, an individual may request that an electronic copy of her PHI be provided to her in Microsoft (MS) Word; MS Excel; Portable Document Format (PDF); or as structured, machine readable data (e.g., a document following the Consolidated Clinical Document Architecture (CCDA) standard using LOINC (to represent lab tests) and RxNorm (to represent medications)); or other electronic format; and the covered entity must provide the copy in the requested format if readily producible in that format. Further, if the PHI that is the subject of the request is maintained electronically by a covered entity, the entity is required to have the capability to provide some form of electronic copy (see 78 FR 5633, <https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>) – and this means that some covered entities may need to make some investments (which cannot be charged to individuals) in order to meet this baseline requirement. If an individual requests a form of electronic copy that the covered entity is unable to produce, the covered entity must offer other electronic formats that are available on its systems. If the individual declines to accept any of the electronic formats that are readily producible by the covered entity, only then may the covered entity provide a hard copy to fulfill the access request. Thus, individuals who request electronic access to PHI maintained electronically can be diverted to receiving a paper copy only in circumstances where all of the covered entities’ existing capabilities for readily producing electronic copies have been presented to the individual but the individual has determined that those formats are not acceptable to her.

When an individual requests access to PHI in a particular form or format, the question for the covered entity is whether or not the entity is able to readily produce the copy in that format – which is a matter of capability, not “willingness.” Thus, if a covered entity has the capability to readily produce the requested format, it is not permissible for the covered entity to deny the individual access to that format because the entity would prefer that the individual receive a different format, or utilize other customary record access processes of the entity.

# What is the intersection of the HIPAA right of access and the HITECH Act’s Medicare and Medicaid Electronic Health Record Incentive Program’s “View, Download, and Transmit” provisions?

Under the HIPAA Privacy Rule, an individual has the right to access PHI maintained about the individual by a covered entity in a designated record set. This may contain electronic or non-electronic PHI. See 45 CFR 164.524(a)(1).  Under the HITECH Act’s Electronic Health Record (EHR) Incentive Program, eligible professionals, eligible hospitals, and critical access hospitals (CAHs) may receive incentive payments under Medicare and Medicaid and avoid payment reductions under Medicare for successfully demonstrating meaningful use of Certified EHR Technology, which includes providing patients the ability to view online, download, and transmit their health information.  It is important to note that in some respects the EHR Incentive Program contains more exacting standards than the baseline requirements of the HIPAA Privacy Rule, while the HIPAA Privacy Rule contains more comprehensive requirements than the EHR Incentive Program (e.g., the HIPAA Privacy Rule access right applies to electronic and paper records, while the EHR Incentive Program applies to certain electronic records).

Below are some key distinctions between the HIPAA right of access and the individual access opportunities that may be offered through the EHR Incentive Program:

| **EHR Incentive Program** | **HIPAA Privacy Rule** |
| --- | --- |
| Professional or hospital proactively makes available certain information for the patient to view, download, or transmit (more than 50% of patients are provided timely access in Stage 2; more than 80% in Stage 3) | Covered entity required by law to provide individuals with access upon request |
| Access is to a specific set of data (e.g., recent lab test results, current medication list and medication history, problem list)\* maintained in Certified EHR Technology (for Stage 3, the specific set of data is known as the Common Clinical Data Set (CCDS), as defined in the 2015 Edition Health IT Certification Rule\*\*)\*See the EHR Incentive Program Final Rule at 80 FR 62812,<https://www.federalregister.gov/articles/2015/10/16/2015-25595/medicare-and-medicaid-programs-electronic-health-record-incentive-program-stage-3-and-modifications>\*\*See 80 FR 62602,<https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base> | Access is to requested PHI that is in a designated record set which is PHI that is either maintained electronically (e.g., in the EHR) or other medical information that is not stored in the EHR (e.g., PHI that is stored on paper, billing records, and other records used to make decisions about individuals) |
| Access must be timely provided (e.g., in Stage 2, professionals must make information available within 4 business days of its availability to the professional, and hospitals must make information about hospital stays available within 36 hours of discharge; for Stage 3, information must be available to the patient within 48 hours of its availability to a professional and 36 hours of its availability to a hospital) | Prompt access is encouraged but covered entities may take no longer than 30 days from receipt to act on a request for access (and may take another 30 days to respond if the individual is notified in writing of the reason for delay during the initial 30 day period) |
| Administered by the Centers for Medicare & Medicaid Services (with respect to the EHR Incentive Program) and the Office of the National Coordinator for Health IT (with respect to the Health IT Certification Program) | Administered by the HHS Office for Civil Rights |

Although the EHR Incentive Program and the HIPAA Privacy Rule are distinct, it is possible for a provider or hospital to leverage its Certified EHR Technology to fulfill its HIPAA Privacy Rule obligations with respect to individual access in circumstances where the individual either: (1) requests access to PHI that is held in the Certified EHR Technology; or (2) requests access to his PHI, the covered entity professional or hospital informs the individual that the PHI requested is available through the Certified EHR Technology, and the individual agrees to access the requested PHI through the Certified EHR Technology.

In scenario 1, the individual is aware of the EHR Incentive Program and specifically requests access to her PHI via the functionality of the Certified EHR Technology.  For example, in exercising her right of access under the HIPAA Privacy Rule, an individual could request a copy of her information that constitutes the CCDS through the provider’s Certified EHR Technology portal or that it be sent from the Certified EHR Technology to the individual’s Direct address (an electronic address for securely exchanging health information using the Direct technical standard).  If the provider is using Certified EHR Technology, the HIPAA Privacy Rule requires the provider to grant this request from the individual because the form and format requested is “readily producible” using the provider’s Certified EHR Technology.  At the same time, the provider should be able to count this access by the individual for purposes of meeting its EHR Incentive Program objectives, as long as the access was provided within the timeframes required by the EHR Incentive Program.  Because the Privacy Rule provides up to 30 days to act on an access request, meeting the more prompt deadlines of the EHR Incentive Program clearly complies with the Privacy Rule’s deadlines.

In scenario 2, the individual has requested a copy of certain of his PHI, and the provider recognizes that the PHI requested by the individual would be easily available through the Certified EHR Technology.  The individual asks for the information in PDF format; the provider instead offers to set up an account for the individual so that the individual can access this information directly through the portal in the Certified EHR Technology.  If the individual agrees to the portal access, the provider will be able to satisfy the individual’s HIPAA access request using the Certified EHR Technology portal, while at the same time being able to count the access for purposes of meeting EHR Incentive Program objectives (as long as the access was provided within the timeframes required by the EHR Incentive Program).  If the individual declines the offer and instead maintains his request to receive a copy of his PHI in PDF format, the HIPAA Privacy Rule requires the provider to provide the individual with a copy in PDF format, if the PHI is readily producible in that format or, if not, in an alternative electronic format that is agreeable to the patient.  Further, the individual at all times retains the right to access his PHI in a designated record set that is not part of or available through the Certified EHR Technology.

# Does an individual have a right under HIPAA to access his PHI in a particular technical standard?

In some circumstances, an individual may request access to an electronic copy of his PHI in a particular technical standard – for example, a copy of the individual’s medication data represented in RxNorm or a lab test represented in LOINC. An individual may request PHI in a particular standard in order to use that information in other software the individual is using. If the covered entity is able to readily produce the PHI in the requested standard format, the covered entity must do so (unless the entity has a ground for denial as specified in the Privacy Rule at 45 CFR 164.524(a). (We note that individuals, in exercising their rights of access under the Privacy Rule, are not required to state their purpose for requesting access, regardless of whether or not a particular form or format for the request is specified, and an individual’s rationale for requesting access is not a reason to deny access.)

# Do individuals have a right under HIPAA to get copies of their x-rays or other diagnostic images, and if so, in what format?

Yes. An individual has a right to receive PHI about the individual maintained by a covered entity in a designated record set, such as a medical record. See 45 CFR 164.524(a)(1). This includes x-rays or other images in the record. As with other PHI in a designated record set, the individual has a right to access the information in the form and format she requests, as long as the covered entity can readily produce it in that form and format. See 45 CFR 164.524(c). The large file size of some x-rays or other images may impact the mechanism for access (e.g., the format agreed upon by the individual and the covered entity must accommodate the file size).

# Do individuals have the right under HIPAA to have copies of their PHI transferred or transmitted to them in the manner they request, even if the requested mode of transfer or transmission is unsecure?

Yes, as long as the PHI is “readily producible” in the manner requested, based on the capabilities of the covered entity and transmission or transfer in such a manner would not present an unacceptable level of security risk to the PHI on the covered entity’s systems, such as risks that may be presented by connecting an outside system, application, or device directly to a covered entity’s systems (as opposed to security risks to PHI once it has left the systems). For example, individuals generally have a right to receive copies of their PHI by mail or e-mail, if they request. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI once it has left the systems. Thus, a covered entity may not require that an individual travel to the covered entity’s physical location to pick up a copy of her PHI if the individual requests the copy be mailed or e-mailed. In the limited case where a covered entity is unable to e-mail the PHI as requested, such as in the case where diagnostic images are requested and e-mail cannot accommodate the file size of the images, the covered entity should offer the individual alternative means of receiving the PHI, such as on portable media that can be mailed to the individual.

Further, while covered entities are required by the Privacy and Security Rules to implement reasonable safeguards to protect PHI while in transit, individuals have a right to receive a copy of their PHI by unencrypted e-mail if the individual requests access in this manner. In such cases, the covered entity must provide a brief warning to the individual that there is some level of risk that the individual’s PHI could be read or otherwise accessed by a third party while in transit, and confirm that the individual still wants to receive her PHI by unencrypted e-mail. If the individual says yes, the covered entity must comply with the request. We note that providers using the 2015 edition of Certified EHR Technology will have the capability to send unencrypted e-mail transmissions directly from that technology.

Whether an individual has a right to receive a copy of her PHI through other unsecure modes of transmission or transfer (assuming the individual requests the mode and accepts the risk) depends on the extent to which the mode of transmission or transfer is within the capabilities of the covered entity and the mode would not present an unacceptable level of risk to the security of the PHI on the covered entity’s systems (as explained above), based on the covered entity’s Security Rule risk analysis. For example, a covered entity’s risk analysis may provide that connecting an outside (foreign) device, such as a USB drive, directly to the entity’s systems presents an unacceptable level of risk to the PHI on the systems. In this case, the covered entity is not required to agree to an individual’s request to transfer the PHI in this manner, but the entity must offer some other means of providing electronic access to the PHI.

Note that while an individual can receive copies of her PHI by unsecure methods if that is her preference, as described in more detail above, a covered entity is not permitted to require an individual to accept unsecure methods of transmission in order to receive copies of her health information.

# Is a covered entity responsible if it complies with an individual’s access request to receive PHI in an unsecure manner (e.g., unencrypted e-mail) and the information is intercepted while in transit?

No. While covered entities are responsible for adopting reasonable safeguards in implementing the individual’s request (e.g., correctly entering the e-mail address), covered entities are not responsible for a disclosure of PHI while in transmission to the individual based on the individual’s access request to receive the PHI in an unsecure manner (assuming the individual was warned of and accepted the risks associated with the unsecure transmission). This includes breach notification obligations and liability for disclosures that occur in transit. Further, covered entities are not responsible for safeguarding the information once delivered to the individual. Covered entities are responsible for breach notification for unsecured transmissions and may be liable for impermissible disclosures of PHI that occur in all contexts except when fulfilling an individual’s right of access under 45 CFR 164.524 to receive his or her PHI or direct the PHI to a third party in an unsecure manner.

# Do individuals have a right under HIPAA to have their PHI downloaded on portable media that they provide?

Whether PHI is “readily producible” for purposes of providing access will depend on the extent to which the requested method of copying, transfer, or transmission is within the capabilities of the covered entity and would not present an unacceptable level of risk to the security of the PHI on the covered entity’s systems, based on the covered entity’s Security Rule risk analysis.

With respect to portable media supplied by an individual, covered entities are required by the Security Rule to perform a risk analysis related to the potential use of external portable media and are not required to accept the external media if they determine there is an unacceptable level of risk to the PHI on their systems. However, covered entities are not then permitted to require individuals to purchase a portable media device from the covered entity if the individual does not wish to do so. The individual may in such cases opt to receive an alternative form of the electronic copy of the PHI, such as through email.

# Do individuals have a right under HIPAA to have a covered entity establish a direct connection between the covered entity’s system and the individual’s app or device in order to provide the individuals with access to their PHI?

Whether PHI is “readily producible” for purposes of providing access will depend on the extent to which establishing the connection is within the capabilities of the covered entity and would not present an unacceptable level of risk to the security of the PHI on a covered entity’s systems, based on the covered entity’s Security Rule risk analysis.

A covered entity may determine that it has the capability to establish the type of connection requested in a manner consistent with the applicable security measures implemented in accordance with its security management process. In that case, the covered entity must provide access in the manner requested by the individual. Further, we note that starting in 2018, under Stage 3 of the EHR Incentive Program, eligible professionals, eligible hospitals, and critical access hospitals (CAHs) using Certified EHR Technology must enable application programming interface (API) functionality that would allow patients to use the application of their choice to access their data. In addition, we note that many provider systems are already using API functionality to provide patients with access to their data today in a secure manner. We expect that covered entities will assess and address any security considerations associated with connecting their systems with individual applications or devices, including through Certified EHR Technology (where applicable), as part of their HIPAA security management process.

# Does an individual have a right under HIPAA to access their health information in human readable form?

Yes. In general, a covered entity must provide an individual with access to PHI about the individual in a designated record set in the form and format requested by the individual, if it is readily producible in such form and format. In cases where the PHI is not readily producible in the requested form and format, the covered entity must provide the PHI in a readable alternative form and format as agreed to by the covered entity and the individual. See 45 CFR 164.524(c)(2). Thus, individuals have a right under HIPAA to access PHI about themselves in human readable form. In cases where a covered entity is providing an individual with an electronic copy of PHI, we also expect the covered entity to provide the copy in machine readable form (i.e., in a form able to be processed by a computer), to the extent possible and where consistent with the individual’s request.

# Is a health care provider permitted to deny an individual’s request for access because the individual has not paid for health care services provided to the individual?

No. A covered entity may charge an individual that has requested a copy of her PHI a reasonable, cost-based fee for the copy. See 45 CFR 164.524(c)(4). However, a covered entity may not withhold or deny an individual access to her PHI on the grounds that the individual has not paid the bill for health care services the covered entity provided to the individual.

# If an individual’s physician orders a test from a clinical laboratory that may take multiple steps or a series of tests to complete, at what point does the test report become part of the laboratory’s designated record set to which an individual has a right of access?

For purposes of the HIPAA Privacy Rule, clinical laboratory test reports become part of the laboratory’s designated record set when they are “complete,” which means that all results associated with an ordered test are finalized and ready for release.

# Is a clinical laboratory required to provide an individual with access to a test report that is not yet complete?

No. For purposes of the HIPAA Privacy Rule, clinical laboratory test reports become part of the laboratory’s designated record set when they are “complete,” which means that all results associated with an ordered test are finalized and ready for release. However, other information concerning the test may be part of the designated record set and thus, accessible to the individual, even if the test report has not yet been completed, such as test orders, ordering provider information, billing information, and insurance information.

# If an individual requests access from a clinical laboratory to a test report on the individual, is the laboratory required to interpret the test results for the individual?

No. There is no requirement in the HIPAA Privacy Rule that clinical laboratories interpret test results for patients. An individual has a right under the HIPAA Privacy Rule merely to inspect or receive a copy (or direct the copy to a designated third party), upon request, of the completed test reports (as well as other information in the designated record set) maintained by a laboratory that is a covered entity. Laboratories may continue to refer patients with questions about the test results back to their ordering or treating providers. However, while not required, a laboratory providing a test report to an individual that has requested access to the report may also provide educational or explanatory materials regarding the test results to individuals if it chooses to do so. Similarly, a laboratory that wishes to include a disclaimer, caveat, or other statement explaining the limitations of the laboratory data for diagnosis or treatment or other purposes may do so.

# Under HIPAA, when can a family member of an individual access the individual’s PHI from a health care provider or health plan?

The HIPAA Privacy Rule provides individuals with the right to access their medical and other health records from their health care providers and health plans, upon request. The Privacy Rule generally also gives the right to access the individual’s health records to a personal representative of the individual. Under the Rule, an individual’s personal representative is someone authorized under State or other applicable law to act on behalf of the individual in making health care related decisions. With respect to deceased individuals, the individual’s personal representative is an executor, administrator, or other person who has authority under State or other law to act on behalf of the deceased individual or the individual’s estate. Thus, whether a family member or other person is a personal representative of the individual, and therefore has a right to access the individual’s PHI under the Privacy Rule, generally depends on whether that person has authority under State law to act on behalf of the individual. See 45 CFR 164.502(g) and 45 CFR 164.524.

In cases where a family member may not have the requisite authority to be a personal representative, an individual still has the ability, under the HIPAA right of access, to direct a covered entity to transmit a copy of the individual’s PHI to the family member, and the covered entity must comply with the request, except in limited circumstances. The individual’s request must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI. See 45 CFR 164.524(c)(3)(ii).

Outside of the HIPAA right of access, other provisions in the Privacy Rule address disclosures to family members. Specifically, a covered entity is permitted to share information with a family member or other person involved in an individual’s care or payment for care as long as the individual does not object. In cases where the individual is incapacitated, a covered entity may share the individual’s information with the family member or other person if the covered entity determines, based on professional judgment, that the disclosure is in the best interest of the individual. If the individual is deceased, a covered entity may make the disclosure unless doing so is inconsistent with any prior expressed preference of the individual. These disclosures are generally limited to the health information that is relevant to the person’s involvement in the individual’s care or payment for care. See 45 CFR 164.510(b).

Finally, a covered entity also is permitted to disclose the health information about an individual to any person, including a family member, if the individual provides a prior written authorization for the disclosure. See 45 CFR 164.508.

# May a covered entity accept standing requests from individuals to access their PHI or to have their PHI sent to a third party of their choice?

Yes, and covered entities should have processes in place that enable individuals to receive access to their PHI, including to direct a copy of their PHI to a third party of their choice, on a standing, regular basis, without requiring individuals to repeat their requests for access every time a copy of their PHI is to be sent or otherwise made accessible. Further, covered entities should take advantage of technology and tools that automate such regular access.

# How can a covered entity account for the date of access if it is not known for certain?

### Answer:

Accounting for disclosures requires an individual to be informed of the date the disclosure was made ([45 CFR 164.528](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-528.xml)(b)(2)). If access to a universe of records was provided for a discrete period of time, Office for Civil Rights (OCR) interprets this provision to permit the accounting to include the range of dates (e.g., access was provided from August 1 to August 3, 2003; or during the week of August 10, 2003). If the disclosure is routinely made within a set period from an event, OCR, likewise, interprets this provision to permit the accounting to provide the date of the event and the normal interval (e.g., gun shot wound reported within 48 hours of treatment and provide date of treatment; hospital discharges reported on 15th of the following month and provide date of discharge; or access provided to public health authorities within 30 days of treatment in emergency department and provide the date of treatment).

# If I believe that my privacy rights have been violated, when can I submit a complaint?

### Answer:

By law, health care providers (including doctors and hospitals) who engage in certain electronic transactions, health plans, and health care clearinghouses, (collectively, “covered entities”) had until April 14, 2003, to comply with the HIPAA Privacy Rule. (Small health plans had until April 14, 2004, to comply).  OCR provides further information on its web site about [how to file a complaint.](https://www.hhs.gov/hipaa/filing-a-complaint/index.html)

* Activities occurring before April 14, 2003, are not subject to the Office for Civil Rights (OCR) enforcement actions.
* After that date, a person who believes a covered entity is not complying with a requirement of the Privacy Rule may file with OCR a written complaint, either on paper or electronically.
* This complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred.
* The Secretary may waive this 180-day time limit if good cause is shown. See 45 [CFR 160.306 and 164.534](https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html).

In addition, after the compliance dates above, individuals have a right to file a complaint directly with the covered entity. Individuals should refer to the covered entity’s notice of privacy practices for more information about how to file a complaint with the covered entity.

# Does an individual have a right under the HIPAA Privacy Rule to restrict the protected health information his or her health care provider discloses for workers' compensation purposes?

### Answer:

Individuals do not have a right under the Privacy Rule at 45 CFR 164.522(a) to request that a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) restrict a disclosure of protected health information about them for workers’ compensation purposes when that disclosure is required by law or authorized by, and necessary to comply with, a workers’ compensation or similar law. See 45 CFR 164.522(a) and 164.512(a) and (l).

# Does the HIPAA Privacy Rule require hospitals and doctors' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?

### Answer:

No, the Privacy Rule does not require these types of structural changes be made to facilities.

[Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule. The Department does not consider facility restructuring to be a requirement under this standard.

For example, the Privacy Rule does not require the following types of structural or systems changes:

* Private rooms.
* Soundproofing of rooms.
* Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
* Encryption of telephone systems.

Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered entities also may take into consideration the steps that other prudent health care and health information professionals are taking to protect patient privacy.

Examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

* Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.
* In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers may constitute a reasonable safeguard. For example, a large clinic intake area may reasonably use cubicles or shield-type dividers, rather than separate rooms, or providers could add curtains or screens to areas where discussions often occur between doctors and patients or among professionals treating the patient.
* Hospitals could ensure that areas housing patient files are supervised or locked.

# How can a small provider implement the standards in Security Rule?

### Answer:

The Security Rule standards allow any covered entity (including small providers) to use any security measures that help the covered entity to reasonably and appropriately implement the standards to protect electronic health information.  In deciding what security measures to use, a covered entity can take into account its size, capabilities, and costs of security measures. A small provider who is a covered entity would first assess their security risks and vulnerabilities and the mechanisms currently in place to mitigate those risks and vulnerabilities. Following this assessment, they should determine what additional measures, if any, need to be taken to meet the standards; taking into account their capabilities and the cost of those measures. For more information on the implementation of the Security Rule by small providers, please see the [Security Paper Educational Series.](https://www.hhs.gov/sites/default/files/smallprovider.pdf)

# Why is the HIPAA Security Rule needed and what is the purpose of the security standards?

### Answer:

In enacting HIPAA, Congress mandated the establishment of Federal standards for the security of electronic protected health information (e-PHI). The purpose of the Security Rule is to ensure that every covered entity has implemented safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Standards for security are needed because there is a growth in the exchange of protected health information between covered entities as well as non-covered entities. The standards mandated in the Security Rule protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. The Security Rule establishes a Federal floor of standards to ensure the availability, confidentiality and integrity of e-PHI. State laws which provide more stringent standards will continue to apply over and above the new Federal security standards.

Health care providers, health plans and their business associates have a strong tradition of safeguarding private health information. However, in today’s world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the Rule provides clear standards for the protection of e-PHI.

# Does the Security Rule apply to written and oral communications?

### Answer:

No. The standards and specifications of the Security Rule are specific to electronic protected health information (e-PHI). It should be noted however that e-PHI also includes telephone voice response and fax back systems because they can be used as input and output devices for electronic information systems. E-PHI does not include paper-to-paper faxes or video teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission. In contrast, the requirements of the Privacy Rule apply to all forms of PHI, including written and oral.

# Do the standards of the Security Rule require use of specific technologies?

### Answer:

No. The Security standards were designed to be "technology neutral" in order to facilitate use of the latest and most promising technologies that meet the needs of different healthcare organizations. Any regulatory requirement for implementation of specific technologies would bind the health care community to specific systems and/or software that may be superseded by rapidly developing technologies and improvements.

# What is the difference between addressable and required implementation specifications in the Security Rule?

### Answer:

If an implementation specification is described as “required,” the specification must be implemented. The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards. In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification: (a) implement the addressable implementation specifications; (b) implement one or more alternative security measures to accomplish the same purpose; (c) not implement either an addressable implementation specification or an alternative. The covered entity’s choice must be documented. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. For example, a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a covered entity makes regarding addressable specifications must be documented in writing.  The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

# Is the use of encryption mandatory in the Security Rule?

### Answer:

No. The final Security Rule made the use of encryption an addressable implementation specification. See 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii). The encryption implementation specification is addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI. If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate. If the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure and document the rationale for this decision.

# What is encryption?

### Answer:

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text. For more information about encryption , please see [NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.](https://www.hhs.gov/sites/default/files/nist800111.pdf)

# Do the Security Rule requirements for access control, such as automatic logoff, apply to employees who telecommute or have home-based offices if the employees have access to electronic PHI (e-PHI)?

### Answer:

Yes. Covered entities that allow employees to telecommute or work out of home-based offices, and have access to e-PHI, must implement appropriate safeguards to protect the organization’s data. The automatic logoff implementation specification is addressable, and must therefore be implemented if, after an assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its environment. If the entity decides that the logoff implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate. If the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure and document the rationale for this decision. The information access management and access control standards, however, require the covered entity to implement policies and procedures for authorizing access to e-PHI and technical policies and procedures to allow access only to those persons or software programs that have been appropriately granted access rights.

# Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?

### Answer:

The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

# Does the Security Rule require the use of an electronic or digital signature?

### Answer:

No, the Security Rule does not require the use of electronic or digital signatures. However, electronic or digital signatures could be used as a security measure if the covered entity determines their use is reasonable and appropriate.

# Does the Security Rule mandate minimum operating system requirements for the personal computer systems used by a covered entity?

### Answer:

No. The Security Rule was written to allow flexibility for covered entities to implement security measures that best fit their organizational needs. The Security Rule does not specify minimum requirements for personal computer operating systems, but it does mandate requirements for information systems that contain electronic protected health information (e-PHI). Therefore, as part of the information system, the security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications such as audit controls, unique user identification, integrity, person or entity authentication, or transmission security.  Additionally, any known security vulnerabilities of an operating system should be considered in the covered entity’s risk analysis (e.g., does an operating system include known vulnerabilities for which a security patch is unavailable, e.g., because the operating system is no longer supported by its manufacturer).

# Are covered entities required to use the National Institute of Standards and Technology (NIST) guidance documents referred to in the preamble to the final Security Rule (68 Fed. Reg. 8334 (February 20, 2003))?

### Answer:

No. Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization’s implementation activities. While NIST documents were referenced in the preamble to the Security Rule, their use is not required by the Security Rule.

# Does the Security Rule permit a covered entity to assign the same log-on ID or user ID to multiple employees?

### Answer:

No. Under the Security Rule, covered entities, regardless of their size, are required, under § 164.312(a)(2)(i) to “assign a unique name and/or number for identifying and tracking user identity.” A “user” is defined in § 164.304 as a “person or entity with authorized access.” Accordingly, the Security Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that maintains electronic protected health information (e-PHI), so that system access and activity can be identified and tracked by user. This pertains to workforce members within small or large healthcare provider offices, health plans, group health plans, and healthcare clearinghouses.

# What does the Security Rule require a covered entity to do to comply with the Security Incidents Procedures standard?

### Answer:

45 CFR § 164.304 defines security incident as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The Security Incident Procedures standard at § 164.308(a)(6)(i) requires a covered entity to implement policies and procedures to address security incidents. The associated implementation specification for response and reporting at § 164.308(a)(6)(ii) requires a covered entity to identify and respond to suspected or known security incidents, mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes. In order to maintain a flexible, scalable and technology neutral approach to the Security Rule, no single method is identified for addressing security incidents that will apply to all covered entities. As stated in the preamble to the Security Rule, 68 Fed. Reg. 8350 (February 20, 2003), an entity should be able to rely upon the information gathered in complying with the other security standards, for example, its risk assessment and risk management procedures and the Privacy Rule standards, to determine what constitutes a security incident in the context of its business operations. In addressing the Security Incident Procedures standard, a covered entity may consider some of the following questions: what specific actions would be considered security incidents; how will incidents be documented and reported; what information should be contained in the documentation; how often and to whom should incidents be reported; what are the appropriate responses to certain incidents; and whether identifying patterns of attempted security incidents is reasonable and appropriate. When taking into consideration the requirements of § 164.306(a) and (b), and its risk analysis, the covered entity may decide that certain types of attempted or successful security incidents or patterns of attempted or successful incidents warrant different actions.

For example, a covered entity may decide that a “ping” (a request-response utility used to determine whether a specific Internet Protocol (IP) address, or host, exists or is accessible) on the communications network initiated from an external source would require the following actions to comply with the standard; (1) minimal, if any, response; (2) no mitigation actions since no harmful effects were caused by the incident; and (3) brief documentation of the security incident and outcome, such as, a recording of aggregate statistical information. Based on its analysis, the entity may also determine that other types of incidents, such as suspicious patterns of “pings” on the communications network initiated from an external source or a specific malicious security incident would require a more detailed response, mitigation steps, and more detailed documentation of the incident and outcome. While internal reporting of security incidents is an inherent part of security incident policies and procedures, the Security Rule generally does not require a covered entity to report incidents to outside entities. However, § 164.314(a)(2)(i)(C) and (b)(2)(iv) require contracts between a covered entity and a business associate, and plan documents of a group health plan, respectively, to include provisions that require business associates and plan sponsors to report to the covered entity any security incidents of which they become aware. (Note that in certain circumstances a group health plan may not be required to amend its plan documents. See § 164.314(b)(1).)

# Under the Security Rule, must plan sponsors report security incidents to the group health plan? If so, what types of incidents must be reported and what level of detail is required?

### Answer:

Although a plan sponsor may not be a HIPAA covered entity subject to the Security Rule, it would nevertheless be obligated, through its plan documents, to report such security incidents to the group health plan. Specifically, the required implementation specification at § 164.314(b)(2)(iv) requires the plan documents of the group health plan to require the plan sponsor to “report to the group health plan any security incident of which it becomes aware.” (Note that in certain circumstances a group health plan may not be required to amend its plan documents. See § 164.314(b)(1).) The plan documents could serve as the vehicle to establish a plan sponsor’s specific reporting requirements and should be developed to meet the group health plan’s specific needs. The group health plan and its plan sponsor must document the specifics of the reporting, including the frequency, level of detail, format and other relevant considerations (e.g., in aggregate or per incident, weekly or monthly). In addressing this required implementation specification, a group health plan may consider some of the following questions: what specific actions would be considered security incidents; how will incidents be documented and reported; what information should be contained in the documentation; how often and to whom within the covered entity should incidents be reported; what are the appropriate responses to certain incidents; and whether identifying patterns of attempted security incidents is reasonable and appropriate.

For example, in order to determine the detailed content of its plan documents, in taking into consideration the requirements of § 164.306(a) and (b) and its risk analysis, the group health plan may decide that certain types of attempted or successful security incidents or patterns of attempted or successful incidents, such as a “ping” (a request-response utility used to determine whether a specific Internet Protocol (IP) address, or host, exists or is accessible) on the plan sponsor’s communications network initiated from an external source, could be reported to the group health plan in a monthly report that only includes an aggregate number of pings that month. Based on its analysis, the group health plan may also determine that other types of incidents, such as suspicious patterns of “pings” on the plan sponsor’s communications network initiated from an external source, or a specific malicious security incident, would require a detailed report to the group health plan as soon as the plan sponsor becomes aware of them.

# Are we required to “certify” our organization’s compliance with the standards of the Security Rule?

### Answer:

No, there is no standard or implementation specification that requires a covered entity to “certify” compliance. The evaluation standard § 164.308(a)(8) requires covered entities to perform a periodic technical and non-technical evaluation that establishes the extent to which an entity’s security policies and procedures meet the security requirements. The evaluation can be performed internally by the covered entity or by an external organization that provides evaluations or “certification” services. A covered entity may make the business decision to have an external organization perform these types of services. It is important to note that HHS does not endorse or otherwise recognize private organizations’ “certifications” regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a “certification” by an external organization does not preclude HHS from subsequently finding a security violation.

# How will we know if our organization and our systems are compliant with the Security Rule’s requirements?

### Answer:

The purpose of the Security Rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI) that is collected, maintained, used or transmitted by a covered entity. Compliance is different for each organization and no single strategy will serve all covered entities. Covered entities should look to § 164.306 of the Security Rule for guidance to support decisions on how to comply with the standards and implementation specifications contained in §§ 164.308, 164.310, 164.312, 164.314, and 164.316. In general, this includes performing a risk analysis; implementing reasonable and appropriate security measures; and documenting and maintaining policies, procedures and other required documentation. Compliance is not a one-time goal, but an ongoing process. Meeting the requirements set out in the evaluation standard at § 164.308(a)(8) will assist covered entities in maintaining substantial compliance. By performing periodic technical and non-technical evaluations of the information security environment, a covered entity will be able to better ensure the security of e-PHI.

# Is the Security Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) suspended during a national or public health emergency?

### Answer:

No, the Security Rule is not suspended during a national or public health emergency. The Secretary of HHS may waive sanctions and penalties arising from certain provisions of the Privacy Rule under the Project BioShield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act if the President declares an emergency or disaster and the Secretary declares a public health emergency.  However, these provisions have no application to the Security Rule. The Security Rule includes requirements for covered entities to ensure the confidentiality, integrity and availability of all electronic protected health information they create, receive, maintain or transmit. The rule further requires that covered entities protect against any reasonably anticipated threats or hazards to the security or integrity of such information. Other provisions of the Security Rule require covered entities to implement security measures that specifically contemplate emergency conditions. For example, covered entities must have contingency plans that establish policies and procedures for responding to an emergency or other occurrence (fire, system failure and natural disaster) that damages systems that contain e-PHI (45 CFR §164.308(a)(7)(i)). As with all HIPAA-related complaints, the Office for Civil Rights will evaluate complaints that arise during the course of a national or public health emergency on a case-by-case basis and exercise its discretion in taking enforcement action.  For more information on suspension of the Privacy Rule during a national or public health emergency, please see FAQ #1068.

# What does the Security Rule mean by physical safeguards?

### Answer:

Physical safeguards are physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity’s premises or at another location.

# Does the Security Rule allow you to network computers? In other words, are covered entities allowed to connect two computer systems, either within the covered entity, or between two covered entities or between a covered entity and its business associate(s) so that they can exchange information directly?

### Answer:

With regard to networking computers, there is nothing in the Security Rule that prohibits the networking of computers, whether inside the same company, or between two unrelated companies who conduct business together. However, the covered entity must demonstrate that it has evaluated the risks associated with a network connection, and document that it has established all of the safeguards (technical, physical and administrative) that would serve to reasonably protect the information that is exchanged along the network. That will include an assessment of everything from the firewall to the designation and training of the individuals who have access to the data.

# Who enforces the health information privacy and security standards established under the Health Insurance Portability and Accountability Act (HIPAA)?

### Answer:

The HIPAA Privacy and Security Rules are enforced by the Office for Civil Rights (OCR). [View more information about complaints related to concerns about protected health information.](https://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html)

The Office of E-Health Standards and Services within the Centers for Medicare & Medicaid Services (CMS) enforces the Transactions and Code Sets and National Identifiers (Employer and Provider identifiers) regulations of the Health Insurance Portability and Accountability Act (HIPAA). Complaints regarding the Transactions and Code Sets and National Identifiers regulations may be submitted [electronically](https://htct.hhs.gov/aset/) or via [paper form](http://www.cms.hhs.gov/Enforcement/Downloads/HIPAANon-PrivacyComplaintForm.pdf).  CMS also enforces the insurance portability requirements under Title I of HIPAA. [View more information about portability and how to obtain information or assistance.](http://www.cms.hhs.gov/HealthInsReformforConsume/01_Overview.asp)

May a HIPAA covered entity or its business associate disclose protected health information (PHI) for purposes of cybersecurity information-sharing of cyber threat indicators?

No, unless the disclosure is otherwise permitted under the HIPAA Privacy Rule, particularly given that cyber threat indicators do not generally include PHI.

The Cybersecurity Information Sharing Act of 2015 (CISA) describes cyber threat indicators as information that is necessary to describe or identify: malicious reconnaissance; methods of defeating a security control or exploitation of a security vulnerability; a security vulnerability; methods of causing a user with legitimate access to defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; a description of actual or potential harm caused by an incident; any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or any combination thereof.

The disclosure of cyber threat indicators for cyber information sharing is meant to alert other entities and the federal government to possible or actual threats or vulnerabilities to information systems, and to generally describe possible harms from such threats or vulnerabilities. Such information may include, as described above, technical, physical, or administrative specifications regarding threats to such systems, or vulnerabilities in such systems, and a general description of the harm caused by exploitation of these specifications.

The disclosure of PHI generally is not needed to describe such threats or vulnerabilities. Further, HIPAA would not permit such disclosures unless specific conditions provided in the HIPAA Privacy Rule were met, specifically, an authorization from the individual or the requirements of an applicable permission for disclosure under the Rule.

For example, the HIPAA Privacy Rule in 45 CFR § 164.512 permits covered entities and business associates to disclose PHI to law enforcement officials, without the individual’s written authorization, if specific conditions and limitations are met, including:

* To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena (45 CFR 164.512(f)(1)(ii)(A)-(B)).
* To respond to an administrative request, such as an administrative subpoena or investigative demand or other written request from a law enforcement official, that includes or is accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used (45 CFR 164.512(f)(1)(ii)(C)).
* To respond to a request for limited PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person (45 CFR 164.512(f)(2)).
* To respond to a request for PHI about a victim of a crime, and the victim agrees (45 CFR 164.512(f)(3)).
* To report PHI to law enforcement when required by law to do so (45 CFR 164.512(f)(1)(i)).
* To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct (45 CFR 164.512(f)(4)).
* To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity’s premises (45 CFR 164.512(f)(5)).
* When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime (45 CFR 164.512(f)(6)).
* To federal officials authorized to conduct intelligence, counter-intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3)).

Absent a provision in the Rule expressly permitting disclosure of PHI, such as outlined above, an individual’s authorization would be required for the disclosure of the individual’s PHI.

# Can a physician’s office fax patient medical information to another physician’s office?

### Answer:

The HIPAA Privacy Rule permits physicians to disclose protected health information to another health care provider for treatment purposes. This can be done by fax or by other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact the correct one for the other physician’s office, and placing the fax machine in a secure location to prevent unauthorized access to the information. See [45 CFR164.530](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-530.xml)(c).

# How does the HIPAA Privacy Rule change the laws concerning consent for treatment?

### Answer:

The Privacy Rule relates to uses and disclosures of protected health information, not to whether a patient consents to the health care itself. As such, the Privacy Rule does not affect informed consent for treatment, which is addressed by State law.

# Can a pharmacist use protected health information to fill a prescription that was telephoned in by a patient's physician without the patient's written consent if the patient is a new patient to the pharmacy?

### Answer:

Yes. The pharmacist is using the protected health information for treatment purposes, and the HIPAA Privacy Rule does not require [covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) to obtain an individual’s consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

# Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures without the patient's written consent?

### Answer:

Yes. The HIPAA Privacy Rule does not require covered entities to obtain an individual’s consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

# Are health care providers restricted from consulting with other providers about a patient’s condition without the patient’s written authorization?

### Answer:

No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule’s definition of “treatment” and, therefore, is permissible. In addition, a health care provider (or other covered entity) is expressly permitted to disclose protected health information about an individual to a health care provider for that provider’s treatment of the individual. See [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml).

#  Does the HIPAA Privacy Rule restrict pharmacists from giving advice about over-the-counter medicines to customers?

### Answer:

No. A pharmacist may provide advice to customers about over-the-counter medicines. The Privacy Rule permits a covered entity to disclose protected health information about an individual to the individual. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(a)(1)(i).

# May a health care provider disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS)?

### Answer:

Yes, the HIPAA Privacy Rule permits a provider to disclose protected health information to a health plan for the quality-related health care operations of the health plan, provided that the health plan has or had a relationship with the individual who is the subject of the information, and the protected health information requested pertains to the relationship. See [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml)(c)(4). Thus, a provider may disclose protected health information to a health plan for the plan’s Health Plan Employer Data and Information Set (HEDIS) purposes, so long as the period for which information is needed overlaps with the period for which the individual is or was enrolled in the health plan.

# Does the HIPAA Privacy Rule permit a covered entity or its collection agency to communicate with parties other than the patient (e.g., spouses or guardians) regarding payment of a bill?

### Answer:

Yes. The Privacy Rule permits a covered entity, or a business associate acting on behalf of a covered entity (e.g., a collection agency), to disclose protected health information as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made.

Therefore, a covered entity, or its business associate, may contact persons other than the individual as necessary to obtain payment for health care services. See [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml)(c) and the definition of “payment” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml). However, the Privacy Rule requires a covered entity, or its business associate, to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, as well as to abide by any reasonable requests for confidential communications and any agreed-to restrictions on the use or disclosure of protected health information. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(b), [164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(d), and [164.522](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-522.xml).

# Does the HIPAA Privacy Rule prevent reporting to consumer credit reporting agencies or otherwise create any conflict with the Fair Credit Reporting Act (FCRA)?

### Answer:

No. The Privacy Rule’s definition of “payment” includes disclosures to consumer reporting agencies. These disclosures, however, are limited to the following protected health information about the individual: name and address; date of birth; social security number; payment history; and account number. In addition, disclosure of the name and address of the health care provider or health plan making the report is allowed. The covered entity may perform this payment activity directly, or may carry out this function through a third party, such as a collection agency, under a business associate arrangement.

The Privacy Rule permits uses and disclosures by the covered entity or its business associate as may be required by the Fair Credit Reporting Act (FCRA) or other law. Therefore, the Department does not believe there is a conflict between the Privacy Rule and legal duties imposed on data furnishers by FCRA.

# Does the HIPAA Privacy Rule prevent health plans and providers from using debt collection agencies? Does the Privacy Rule conflict with the Fair Debt Collection Practices Act?

### Answer:

The Privacy Rule permits covered entities to continue to use the services of debt collection agencies. Debt collection is recognized as a payment activity within the “payment” definition. See the definition of “payment” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml). Through a business associate arrangement, the covered entity may engage a debt collection agency to perform this function on its behalf. Disclosures to collection agencies are governed by other provisions of the Privacy Rule, such as the business associate and minimum necessary requirements.

The Department is not aware of any conflict between the Privacy Rule and the Fair Debt Collection Practices Act. Where a use or disclosure of protected health information is necessary for the covered entity to fulfill a legal duty, the Privacy Rule would permit such use or disclosure as required by law.

# Does the HIPAA Privacy Rule permit an eye doctor to confirm a contact prescription received by a mail-order contact company?

### Answer:

Yes. The disclosure of protected health information by an eye doctor to a distributor of contact lenses for the purpose of confirming a contact lens prescription is a treatment disclosure, and is permitted under the Privacy Rule at [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml).

# Does a physician need a patient's written authorization to send a copy of the patient's medical record to a specialist or other health care provider who will treat the patient?

### Answer:

No. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual’s authorization, to another health care provider for that provider’s treatment of the individual. See [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml) and the definition of “treatment” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml).

# Is a hospital permitted to contact another hospital or health care facility, such as a nursing home, to which a patient will be transferred for continued care, without the patient's authorization?

### Answer:

Yes. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual’s authorization, to another health care provider for that provider’s treatment or payment purposes, as well as to another covered entity for certain health care operations of that entity. See [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml) and the definitions of “treatment,” “payment,” and “health care operations” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml).

# When an ambulance service delivers a patient to a hospital, is it permitted to report its treatment of the patient and patient's medical history to the hospital, without the patient's authorization?

### Answer:

Yes. The HIPAA Privacy Rule permits an ambulance service or other health care provider to disclose protected health information about an individual, without the individual’s authorization, to another health care provider, such as a hospital, for that provider’s treatment of the individual. See [45 CFR 164.506](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-506.xml)and the definition of “treatment” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml).

# Does the Privacy Rule permit health plans to disclose protected health information to pharmaceutical manufacturers for the adjudication of drug rebate contracts?

### Answer:

Yes. The Privacy Rule permits a health plan to disclose protected health information, such as prescription numbers, to a pharmaceutical manufacturer for purposes of adjudicating claims submitted under a drug rebate contract. Because the amount of the rebate is based on drug utilization by individual enrollees, such disclosures are permitted as part of a [covered entity](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html)’s payment activities. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(a)(1)(ii) and the definition of “payment” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml).

A business associate agreement is not required to make these disclosures. However, a health plan must make reasonable efforts to limit the information disclosed to that which is the minimum necessary to adjudicate claims under the contract. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(b) and [164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(d) for more information on the minimum necessary standard.

Does the HIPAA Privacy Rule permit a doctor, laboratory, or other health care provider to share patient health information for treatment purposes by fax, e-mail, or over the phone?

Answer:

Yes. The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise.

For example:

* A laboratory may fax, or communicate over the phone, a patient’s medical test results to a physician.
* A physician may mail or fax a copy of a patient’s medical record to a specialist who intends to treat the patient.
* A hospital may fax a patient’s health care instructions to a nursing home to which the patient is to be transferred.
* A doctor may discuss a patient’s condition over the phone with an emergency room physician who is providing the patient with emergency care.
* A doctor may orally discuss a patient’s treatment regimen with a nurse who will be involved in the patient’s care.
* A physician may consult with another physician by e-mail about a patient’s condition.
* A hospital may share an organ donor’s medical information with another hospital treating the organ recipient.

The Privacy Rule requires that covered health care providers apply reasonable safeguards when making these communications to protect the information from inappropriate use or disclosure. These safeguards may vary depending on the mode of communication used. For example, when faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard may involve a provider first confirming the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information. When discussing patient health information orally with another provider in proximity of others, a doctor may be able to reasonably safeguard the information by lowering his or her voice.

# Are appointment reminders allowed under the HIPAA Privacy Rule without authorizations?

### Answer:

Yes, appointment reminders are considered part of treatment of an individual and, therefore, can be made without an authorization.

# Does the HIPAA Privacy Rule permit a health care provider to disclose an injured or ill worker's protected health information without his or her authorization when requested for purposes of adjudicating the individual's workers' compensation claim?

### Answer:

[Covered entities](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html) are permitted to disclose protected health information for such purposes as authorized by, and to the extent necessary to comply with, workers’ compensation law. See 45 CFR 164.512(l). In addition, the Privacy Rule generally permits covered entities to disclose protected health information in the course of any judicial or administrative proceeding in response to a court order, subpoena, or other lawful process. See 45 CFR 164.512(e).

# My state law says I may disclose records, relating to the treatment I provided to an injured worker, to a workers' compensation insurer for purposes of determining the amount of or entitlement to payment under the workers' compensation system. Am I allowed to share this information under the HIPAA Privacy Rule?

### Answer:

Yes. A [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) is permitted to disclose an individual’s protected health information as necessary to comply with and to the full extent authorized by workers’ compensation law. See [45 CFR 164.512(l).](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-workers-compensation/index.html)

# My state law says I may provide information regarding an injured workers' previous condition, which is not directly related to the claim for compensation, to an employer or insurer if I obtain the workers' written release. Am I permitted to make this disclosure under the HIPAA Privacy Rule?

### Answer:

A [covered entity](http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp) may disclose protected health information where the individual’s written authorization has been obtained, consistent with the Privacy Rule’s requirements at [45 CFR 164.508](http://akatest3-ion-www.hhs.gov.edgekey-staging.net/ocr/privacy/hipaa/understanding/special/research/index.html). Thus, a covered entity would be permitted to make the above disclosure if the individual signed such an authorization.

# Is a health care provider permitted to disclose proof of a child’s immunizations directly to a school without a HIPAA authorization?

### Answer:

Yes, provided the school is required by law to have proof of immunizations in order to admit the child, and a parent, guardian, or other person acting *in loco parentis* has agreed to the disclosure.  See 45 CFR 164.512(b)(1)(vi).  Where the individual who is a student or prospective student is an adult or emancipated minor, the provider may make the disclosure with the agreement of the student herself.  In either case, the agreement may be obtained orally or in writing, but must be documented (e.g., by placing in the medical record a copy of a written request, or notation of an oral request, from a parent for the provider to disclose the proof of immunization to the school).

# What type or form of documentation of parental agreement is required under the Privacy Rule in order for a health care provider to be permitted to disclose proof of a child’s immunizations to a school that is subject to a school entry law? For how long must such documentation be maintained?

### Answer:

The Privacy Rule does not prescribe the nature and form of the documentation, allowing covered entities the flexibility to determine what is appropriate for their purposes and to address the varied circumstances in which parental agreement may be obtained.  The documentation must only make clear that agreement was obtained as required by 45 CFR 164.512(b)(1)(vi) of the Privacy Rule.  For example, if a parent or guardian submits a written or email request to a covered entity to disclose proof that his or her child has been immunized to the child’s school, a copy of the request would suffice as documentation of the agreement.  Likewise, if a parent or guardian calls the covered entity and requests over the phone that proof of his or her child’s immunization be disclosed to the child’s school, a notation in the child’s medical record or elsewhere of the phone call would suffice as documentation of the agreement.  The documentation for these purposes need not include the signature of a parent or guardian or any of the other elements required under the Privacy Rule for a written HIPAA authorization.  As with other documentation required under the Privacy Rule, documentation of parental agreement for these purposes must be maintained for six years.  See 45 CFR 164.530(j).

# Where a parent requests that a health care provider disclose proof of his child’s immunizations to a school so the school can legally admit the child, does the Privacy Rule limit to whom at the school the provider may send the records?

### Answer:

No.  It is expected that in most cases a school has designated an administrative official or employee, such as a school nurse, to receive and maintain proof of student immunizations to comply with applicable law. Given the designated person may vary from school to school, the Privacy Rule permits the health care provider to make the disclosure to whoever at the school is identified in the parent’s request or school’s instructions to the parent.

# Must a health care provider obtain a parent’s agreement before each disclosure of proof of a child’s immunization to a school that is required by a school entry law to have such information?

### Answer:

In most cases, it is anticipated that a health care provider will obtain agreement for the disclosure of proof of immunization to a school at the time a particular disclosure is needed.  For example, a parent may call and request that a covered health care provider send proof of his or her child’s immunizations to an elementary school before the child is to begin school.  If that child moves to a different school and is unable to transfer the immunization records to the new school, the parent may then need to request that the health care provider send the child’s records directly to the new school.  However, in some circumstances the scope of the agreement may vary based on the needs of the parent and the school.  For example, a parent may agree to the health care provider making multiple disclosures over a period of time, such as where updates are required by a school when a series of vaccinations have been completed.

# If a state law requires a covered health care provider to disclose proof of a student’s immunizations directly to a school without the affirmative permission of a parent or guardian, must the health care provider also obtain the agreement of a parent or guardian in accordance with 45 CFR 164.512(b)(1)(vi) of the Privacy Rule prior to making the disclosure?

### Answer:

No.  The Privacy Rule permits a covered entity to use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of that law.  See 45 CFR 164.512(a).  In such cases, the covered entity is not required to also meet the conditions of 45 CFR 164.512(b)(1)(vi) in making the required by law disclosure.

# Under the student immunization disclosure provisions at 45 CFR 164.512(b)(1)(vi), is a health care provider permitted to disclose proof of a child’s immunization to a school that is not subject to a school entry law with respect to the information?

### Answer:

No, 45 CFR 164.512(b)(1)(vi) of the Privacy Rule permits the disclosure of proof of immunization about a student or prospective student only to a school that is required by State or other law to have such information prior to admitting the student.  In the limited case where a school is not subject to a school entry law but seeks proof of immunization of students, a covered health care provider may either provide the proof of immunization to the parent of the student (or student, if applicable) to give to the school, or obtain the parent’s (or student’s, if applicable) written authorization to provide the requested information directly to the school.

# Does the HIPAA Privacy Rule require schools to maintain student immunization records?

### Answer:

No; however, State or other applicable laws may impose retention requirements for such records.  Further, in most cases, the Privacy Rule will not provide protections to the immunization records maintained by a school because: (1) the school is not a HIPAA covered entity; or (2) the records are maintained by an educational institution or agency to which the Family Educational Rights and Privacy Act (FERPA) applies and, thus, are protected by FERPA and not HIPAA.

# How does the HIPAA Privacy Rule apply to professional liability insurance? Specifically, how can professional liability insurers continue to arrange for and maintain medical liability insurance for health care providers covered by the Rule?

### Answer:

# The Privacy Rule permits a covered health care provider to disclose information for “health care operations” purposes, subject to certain requirements. Disclosures by a covered health care provider to a professional liability insurer or a similar entity for the purpose of obtaining or maintaining medical liability coverage or for the purpose of obtaining benefits from such insurance, including the reporting of adverse events, fall within “business management and general administrative activities” under the definition of “health care operations.” Therefore, a covered health care provider may disclose individually identifiable health information to a professional liability insurer to the same extent as the provider is able to disclose such information for other health care operations purposes.Does the Privacy Rule permit state Medicaid agencies to disclose protected health information to pharmaceutical manufacturers and third party data vendors for purposes of validating claims under the Medicaid Drug Rebate program?

### Answer:

Yes. The Privacy Rule permits State Medicaid agencies to disclose protected health information, such as prescription numbers, to pharmaceutical manufacturers and third party data vendors that assist the pharmaceutical manufacturers, for purposes of validating claims submitted under the Medicaid Drug Rebate program. Because the amount of the rebate is based on drug utilization by individual enrollees, such disclosures are permitted as part of a State Medicaid agency’s payment activities. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(a)(1)(ii) and the definition of “payment” at [45 CFR 164.501](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-501.xml).

A business associate agreement is not required to make these disclosures. State Medicaid agencies are required by law to disclose certain information to drug manufacturers as part of the drug rebate program. To the extent that the law requires a disclosure, the minimum necessary standard does not apply. (See [45 CFR 164.512](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-512.xml)(a) for further information and limitations on disclosures required by law.) To the extent that protected health information is disclosed for payment purposes but not pursuant to a legal requirement, the State Medicaid agency must make reasonable efforts to limit that information to that which is the minimum necessary to adjudicate the rebate claims. See [45 CFR 164.502](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-502.xml)(b) and [164.514](https://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec164-514.xml)(d) for more information on the minimum necessary standard.

# May a Medicaid state agency and a Medicare Advantage plan share protected health information to identify dually eligible enrollees?

### Answer:

Yes. The HIPAA Privacy Rule permits a covered entity to disclose protected health information (PHI) both for its own payment purposes, as well as for the payment purposes of another covered entity that receives the information. See 45 CFR 164.506(c)(3). The Privacy Rule defines “payment” to include activities to determine eligibility or coverage of enrollees. See the definition of “payment” at 45 CFR 164.501, paragraph (2)(i). Thus, a Medicaid State agency and a Medicare Advantage plan may disclose to each other PHI about their enrollees to identify those enrollees that are dually eligible under both plans. Such disclosures must comport with the Privacy Rule’s minimum necessary standard, where applicable. See 45 CFR 164.502(b), 164.514(d). In general, an electronic inquiry and response from one health plan to another to obtain information regarding the eligibility of an enrollee to receive health care must be done using the HIPAA standard transaction for eligibility (X12N 270/271 transaction). Where the disclosures between the State Medicaid agency and the Medicare Advantage plan are conducted using the standard, the Privacy Rule’s minimum necessary requirements do not apply to the disclosures of the data elements required or situationally required by the standard transaction. In contrast, where the disclosures are made outside of a standard transaction, both the Medicare Advantage plan in its request for PHI, as well as the State Medicaid agency in its response, must make reasonable efforts to limit the PHI requested and disclosed to the minimum necessary PHI for the purpose of identifying dually eligible enrollees. Because the Medicare Advantage plan must limit its request to the minimum necessary PHI to identify dually eligible enrollees, the State Medicaid agency may rely, if reasonable, on that request for PHI as satisfying the minimum necessary requirement for these purposes. See 45 CFR 164.514(d)(3)(iii).