

CONSENT

[45 CFR § 164.506]

Background

The Privacy Rule establishes a federal requirement that most doctors, hospitals, or other health care providers obtain a patient's written consent before using or disclosing the patient's personal health information to carry out treatment, payment, or health care operations (TPO). Today, many health care providers, for professional or ethical reasons, routinely obtain a patient's consent for disclosure of information to insurance companies or for other purposes. The Privacy Rule builds on these practices by establishing a uniform standard for certain health care providers to obtain their patients' consent for uses and disclosures of health information about the patient to carry out TPO.

General Provisions

- Patient consent is required before a covered health care provider that has a direct treatment relationship with the patient may use or disclose protected health information (PHI) for purposes of TPO. Exceptions to this standard are shown in the next bullet.
- Uses and disclosures for TPO may be permitted without prior consent in an emergency, when a provider is required by law to treat the individual, or when there are substantial communication barriers.
- Health care providers that have indirect treatment relationships with patients (such as laboratories that only interact with physicians and not patients), health plans, and health care clearinghouses may use and disclose PHI for purposes of TPO without obtaining a patient's consent. The rule permits such entities to obtain consent, if they choose.
- If a patient refuses to consent to the use or disclosure of their PHI to carry out TPO, the health care provider may refuse to treat the patient.
- A patient's written consent need only be obtained by a provider one time.
- The consent document may be brief and may be written in general terms. It must be written in plain language, inform the individual that information may be used and disclosed for TPO, state the patient's rights to review the provider's privacy notice, to request restrictions and to revoke consent, and be dated and signed by the individual (or his or her representative).

Individual Rights

- An individual may revoke consent in writing, except to the extent that the covered entity has taken action in reliance on the consent.
- An individual may request restrictions on uses or disclosures of health information for TPO. The covered entity need not agree to the restriction requested, but is bound by any restriction to which it agrees.
- An individual must be given a notice of the covered entity's privacy practices and may review that notice prior to signing a consent.

Administrative Issues

- A covered entity must retain the signed consent for 6 years from the date it was last in effect. The Privacy Rule does not dictate the form in which these consents are to be retained by the covered entity.
- Certain integrated covered entities may obtain one joint consent for multiple entities.
- If a covered entity obtains consent and also receives an authorization to disclose PHI for TPO, the covered entity may disclose information only in accordance with the more restrictive document, unless the covered entity resolves the conflict with the individual.
- Transition provisions allow providers to rely on consents received prior to April 14, 2003 (the compliance date of the Privacy Rule for most covered entities), for uses and disclosures of health information obtained prior to that date.

Q: Will the consent requirement restrict the ability of providers to consult with other providers about a patient's condition?

A: No. A provider with a direct treatment relationship with a patient would have to have initially obtained consent to use that patient's health information for treatment purposes. Consulting with another health care provider about the patient's case falls within the definition of "treatment" and, therefore, is permissible. If the provider being consulted does not otherwise have a direct treatment relationship with the patient, that provider does not need to obtain the patient's consent to engage in the consultation.

Q: Does a pharmacist have to obtain a consent under the Privacy Rule in order to provide advice about over-the-counter medicines to customers?

A: No. A pharmacist may provide advice about over-the-counter medicines without obtaining the customers' prior consent, provided that the pharmacist does not create or keep a record of any PHI. In this case, the only interaction or disclosure of information is a conversation between the pharmacist and the customer. The pharmacist may disclose PHI about the customer to the customer without obtaining his or her consent (§ 164.502(a)(1)(i)), but may not otherwise use or disclose that information.

Q: **The rule provides an exception to the prior consent requirement for “emergency treatment situations.” How will a provider know when the situation is an “emergency treatment situation” and, therefore, is exempt from the Privacy Rule’s prior consent requirement?**

A: Health care providers must exercise their professional judgment to determine whether obtaining a consent would interfere with the timely delivery of necessary health care. If, based on professional judgment, a provider reasonably believes at the time the patient presents for treatment that a delay involved in obtaining the patient’s consent to use or disclose information would compromise the patient’s care, the provider may use or disclose PHI that was obtained during the emergency treatment, without prior consent, to carry out TPO. The provider must attempt to obtain consent as soon as reasonably practicable after the provision of treatment. If the provider is able to obtain the patient’s consent to use or disclose information before providing care, without compromising the patient’s care, we require the provider to do so.

Q: **Does the exception to the consent requirement regarding substantial barriers to communication with the individual affect requirements under Title VI of the Civil Rights Act of 1964 or the Americans with Disabilities Act?**

A: No. The provision of the Privacy Rule regarding substantial barriers to communication does not affect covered entities’ obligations under Title VI or the Americans with Disabilities Act. Entities that are covered by these statutes must continue to meet the requirements of the statutes. The Privacy Rule works in conjunction with these laws to remove impediments to access to necessary health care for all individuals.

Q: **What is the difference between “consent” and “authorization” under the Privacy Rule?**

A: A consent is a general document that gives health care providers, which have a direct treatment relationship with a patient, permission to use and disclose all PHI for TPO. It gives permission only to that provider, not to any other person. Health care providers may condition the provision of treatment on the individual providing this consent. One consent may cover all uses and disclosures for TPO by that provider, indefinitely. A consent need not specify the particular information to be used or disclosed, nor the recipients of disclosed information.

Only doctors or other health care providers with a direct treatment relationship with a patient are required to obtain consent. Generally, a “direct treatment provider” is one that treats a patient directly, rather than based on the orders of another provider, and/or provides health

care services or test results directly to patients. Other health care providers, health plans, and health care clearinghouses may use or disclose information for TPO without consent, or may choose to obtain a consent.

An authorization is a more customized document that gives covered entities permission to use specified PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. Covered entities may not condition treatment or coverage on the individual providing an authorization. An authorization is more detailed and specific than a consent. It covers only the uses and disclosures and only the PHI stipulated in the authorization; it has an expiration date; and, in some cases, it also states the purpose for which the information may be used or disclosed.

An authorization is required for use and disclosure of PHI not otherwise allowed by the rule. In general, this means an authorization is required for purposes that are not part of TPO and not described in § 164.510 (uses and disclosures that require an opportunity for the individual to agree or to object) or § 164.512 (uses and disclosures for which consent, authorization, or an opportunity to agree or to object is not required). Situations in which an authorization is required for TPO purposes are identified and discussed in the next question.

All covered entities, not just direct treatment providers, must obtain an authorization to use or disclose PHI for these purposes. For example, a covered entity would need an authorization from individuals to sell a patient mailing list, to disclose information to an employer for employment decisions, or to disclose information for eligibility for life insurance. A covered entity will never need to obtain both an individual's consent and authorization for a single use or disclosure. However, a provider may have to obtain consent and authorization from the same patient for different uses or disclosures. For example, an obstetrician may, under the consent obtained from the patient, send an appointment reminder to the patient, but would need authorization from the patient to send her name and address to a company marketing a diaper service.

[July 6 Q&A, Concerning When An Authorization Would Be Required For Uses and Disclosures for TPO, Removed on January 14, 2002**]**

Q: Will health care providers be required to determine whether another covered entity has a more restrictive consent form before disclosing information to that entity for TPO purposes?

A: No. Generally, a consent permits only the covered entity that obtains the consent to use or disclose PHI for its own TPO purposes. Under the Privacy Rule, one covered entity is not bound by a consent or any restrictions on that consent agreed to by another covered entity, with one exception. A covered entity would be bound by the consent of another covered entity if the

entities use a “joint consent,” as permitted by the Privacy Rule (§ 164.506(f)).

In addition, it is possible for several entities to choose to be treated as a single covered entity under the rule, as “affiliated entities.” Because affiliated entities are considered to be one covered entity under the rule, there would be only one consent and each entity would be bound by that consent (§ 164.504(d)).

Q: What is the interaction between “consent” and “notice”?

A: The consent and the notice of privacy practices are two distinct documents. A consent document is brief (may be less than one page). It must refer to the notice and must inform the individual that he has the opportunity to review the notice prior to signing the consent. The Privacy Rule does not require that the individual read the notice or that the covered entity explain each item in the notice before the individual provides consent. We expect that some patients will simply sign the consent while others will read the notice carefully and discuss some of the practices with the covered entity.

Q: May consent for use or disclosure of PHI be provided electronically?

A: Yes. The covered entity may choose to obtain and store consents in paper or electronic form, provided that the consent meets all of the requirements under the Privacy Rule, including that it be signed by the individual. Paper is not required.

Q: Must a covered entity verify a signature on a consent form if the individual is not present when he signs it?

A: No.

Q: May consent be obtained by a health care provider only one time if there is a single connected course of treatment involving multiple visits?

A: Yes. A health care provider needs to obtain consent from a patient for use or disclosure of PHI only one time. This is true regardless of whether there is a connected course of treatment or treatment for unrelated conditions. A provider will need to obtain a new consent from a patient only if the patient has revoked the consent between treatments.

Q: If an individual consents to the use or disclosure of PHI for TPO purposes, obtains a health care service, and then revokes consent before the provider bills for such service, is the provider precluded from billing for such service?

A: No. A health care provider that provides a health care service to an individual after

obtaining consent from the individual, may bill for such service even if the individual immediately revokes consent after the service has been provided. The Privacy Rule requires that an individual be permitted to revoke consent, but provides that the revocation is not effective to the extent that the health care provider has acted in reliance on the consent. Where the provider has obtained a consent and provided a health care service pursuant to that consent with the expectation that he or she could bill for the service, the health care provider has acted in reliance on the consent. The revocation would not interfere with the billing or reimbursement for that care.

Q: If covered providers that are affiliated or part of an organized health care arrangement are located in different states with different laws regarding uses and disclosures of health information (e.g., a chain of pharmacies), do they need to obtain a consent in each state that the patient obtains treatment?

A: No. The consent is general and only needs to be obtained by a covered entity (or by affiliated entities or entities that are part of an organized health care arrangement) one time. The Privacy Rule does not require that the consent include any details about state law, and therefore, does not require different consent forms in each state. State law may impose additional requirements for consent forms on covered entities.

Q: Must a revocation of a consent be in writing?

A: Yes.

Q: The Privacy Rule permits a covered entity to continue to use or disclose health information which it has on the compliance date pursuant to express legal permission obtained from an individual prior to the compliance date. Is a form, signed by a patient prior to the compliance date of the rule, that permits a provider to use or disclose information for the limited purpose of payment sufficient to meet these transition provision requirements?

A: Yes. A provider that obtains permission from a patient prior to the compliance date to use or disclose information for payment purposes may use the PHI about that patient collected pursuant to that permission for purposes of TPO. Under the transition provisions, if prior to the compliance date, a provider obtained a consent for the use or disclosure of health information for any one of the TPO purposes, the provider may use the health information collected pursuant to that consent for all three purposes after the compliance date (§ 164.532(b)). Thus, a provider that obtained consent for use or disclosure for billing purposes would be able to draw on the data obtained prior to the compliance date and covered by the consent form for all TPO activities to the extent not expressly excluded by the terms of the consent.

Q: Are health plans and health care clearinghouses required by the Privacy Rule to have some form of express legal permission to use and disclose health information obtained prior to the compliance date for TPO purposes?

A: No. Health plans and health care clearinghouses are not required to have express legal permission from individuals to use or disclose health information obtained prior to the compliance date for their own TPO purposes.

PARENTS AND MINORS

[45 CFR § 164.502(g)]

General Requirements

The Privacy Rule provides individuals with certain rights with respect to their personal health information, including the right to obtain access to and to request amendment of health information about themselves. These rights rest with that individual, or with the “personal representative” of that individual. In general, a person's right to control protected health information (PHI) is based on that person's right (under state or other applicable law, e.g., tribal or military law) to control the health care itself.

Because a parent usually has authority to make health care decisions about his or her minor child, a parent is generally a “personal representative” of his or her minor child under the Privacy Rule and has the right to obtain access to health information about his or her minor child. This would also be true in the case of a guardian or other person acting *in loco parentis* of a minor.

There are exceptions in which a parent might not be the “personal representative” with respect to certain health information about a minor child. In the following situations, the Privacy Rule defers to determinations under other law that the parent does not control the minor’s health care decisions and, thus, does not control the PHI related to that care.

- When state or other law does not require 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, the parent is not the minor’s personal representative under the Privacy Rule. For example, when a state law provides an adolescent the right to consent to mental health treatment without the consent of his or her parent, and the adolescent obtains such treatment without the consent of the parent, the parent is not the personal representative under the Privacy Rule for that treatment. The minor may choose to involve a parent in these health care decisions without giving up his or her right to control the related health information. Of course, the minor may always have the parent continue to be his or her personal representative even in these situations.
- When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor, the parent is not the personal representative of the minor for the relevant services. For example, courts may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself. In order to not undermine these court decisions, the parent is not the personal representative

under the Privacy Rule in these circumstances.

In the following situations, the Privacy Rule reflects current professional practice in determining that the parent is not the minor's personal representative with respect to the relevant PHI:

- When a parent agrees to a confidential relationship between the minor and the physician, the parent does not have access to the health information related to that conversation or relationship. For example, if a physician asks the parent of a 16-year old if the physician can talk with the child confidentially about a medical condition and the parent agrees, the parent would not control the PHI that was discussed during that confidential conference.
- When a physician (or other covered entity) reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

Relation to State Law

In addition to the provisions (described above) tying the right to control information to the right to control treatment, the Privacy Rule also states that it does not preempt state laws that specifically address disclosure of health information about a minor to a parent (§ 160.202). This is true whether the state law authorizes or prohibits such disclosure. Thus, if a physician believes that disclosure of information about a minor would endanger that minor, but a state law requires disclosure to a parent, the physician may comply with the state law without violating the Privacy Rule. Similarly, a provider may comply with a state law that requires disclosure to a parent and would not have to accommodate a request for confidential communications that would be contrary to state law.

Frequently Asked Questions

Q: Does the Privacy Rule allow parents the right to see their children's medical records?

A: The Privacy Rule generally allows parents, as their minor children's personal representatives, to have access to information about the health and well-being of their children when state or other underlying law allows parents to make treatment decisions for the child. There are two exceptions: (1) when the parent agrees that the minor and the health care provider may have a confidential relationship, the provider is allowed to withhold information

from the parent to the extent of that agreement; and (2) when the provider reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the provider is permitted not to treat the parent as the child's personal representative with respect to health information.

Secretary Thompson has stated that he is reassessing these provisions of the regulation.

Q: Does the Privacy Rule provide rights for children to be treated without parental consent?

A: 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 health information, not the underlying treatment.

Q: 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?

A: Generally, yes. Even though the parent did not provide consent to the treatment in this situation, under the Privacy Rule, the parent would still be the child's personal representative. This would not be so only when the minor provided consent (and no other consent is required) or the treating physician suspects abuse or neglect or reasonably believes that releasing the information to the parent will endanger the child.