HIPAA PRIVACY PRACTICES FREQUENTLY ASKED QUESTIONS

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.

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. See45 CFR 164.506.

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.

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 and the definition of "treatment" at 45 CFR 164.501.

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.

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?

Answer:

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.

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.

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

Answer:

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?

Answer:

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.

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?

Answer:

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.

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.

- 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.

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 apply to an elementary or secondary school?

Answer:

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 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*,

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. 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.

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 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(h).

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.

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.

Can a CE (health care provider or health plan) share health information with a family member or a friend?

Answer:

HIPAA requires most doctors, nurses, hospitals, nursing homes, and other health care providers to protect the privacy of your health information. However, if you don't object, a health care provider or health plan may share relevant information with family members or friends involved in your health care or payment for your health care in certain circumstances.

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(c) and the definition of "payment" at 45 CFR 164.501. 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(b),164.514(d), and 164.522.

Other circumstances when health information can be shared:

Under HIPAA, your health care provider may share your information face-to-face, over the phone, or in writing. A health care provider or health plan may share relevant information if:

- You give your provider or plan permission to share the information.
- You are present and do not object to sharing the information.
- You are not present, and the provider determines based on professional judgment that it's in your best interest.

Examples:

- An emergency room doctor may discuss your treatment in front of your friend when you ask your friend to come into the treatment room. Your hospital may discuss your bill with your daughter who is with you and has a question about the charges, if you do not object.
- 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 not discuss your condition with your brother if you tell her not to.
- HIPAA also allows health care providers 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.
- A health care provider or health plan may also share relevant information if you are not around or cannot give permission when a health care provider or plan representative believes, based on professional judgment, that sharing the information is in your best interest.

Permitted Uses and Disclosures: Exchange for Health Care Operations

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Permitted Uses and Disclosures: Health Care Operations Examples (January 2016)
45 Code of Federal Regulations (CFR) 164.506(c)(4)

The Health Insurance Portability and Accountability Act (HIPAA) governs how Covered Entities (CEs) protect and secure Protected Health Information (PHI). HIPAA also provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities *without first obtaining* an individual's authorization: including for **treatment and for health care operations** of the disclosing CE or the recipient CE when the appropriate relationship exists.

Other laws may apply. This fact sheet discusses only HIPAA.

Under HIPAA**,** a CE can disclose (whether orally, on paper, by fax, or electronically) PHI *to another CE or that CE's business associate* for the following subset of health care operations activities of the *recipient* CE (45 CFR 164.501) without needing patient consent or authorization (45 CFR 164.506(c)(4)):

1. Conducting quality assessment and improvement activities
2. Developing clinical guidelines
3. Conducting patient safety activities as defined in applicable regulations
4. Conducting population-based activities relating to improving health or reducing health care cost
5. Developing protocols
6. Conducting case management and care coordination (including care planning)
7. Contacting health care providers and patients with information about treatment alternatives
8. Reviewing qualifications of health care professionals
9. Evaluating performance of health care providers and/or health plans
10. Conducting training programs or credentialing activities
11. Supporting fraud and abuse detection and compliance programs.

In general, before a CE can share PHI with another CE for one of the reasons noted above, the following three requirements must also be met:

1. Both CEs must have or have had a relationship with the patient (can be a past or present patient)
2. The PHI requested must pertain to the relationship
3. The discloser must disclose only the minimum information necessary for the health care operation at hand.

Under HIPAA's minimum necessary provisions, a health care provider (hereafter "provider") must make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure or request. (45 CFR 164.502(b)). For example, in sharing information with an individual's health plan for population health programs (for example, a diabetes management program), a provider should disclose the PHI that is necessary for the program to be effective.

For more information see:

www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.