

The logo for the Health Privacy Project, featuring the words "HEALTH", "PRIVACY", and "PROJECT" stacked vertically in white, uppercase, sans-serif font within a solid purple square.

HEALTH PRIVACY PROJECT

MYTHS AND FACTS ABOUT THE HIPAA PRIVACY RULE

Since April 14, 2003, health care providers, health plans, and health care clearinghouses have been required to be in compliance with the HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule. Both the 1996 Congress and the two recent administrations agree that a privacy law is needed to ensure that sensitive personal health information can be shared for core health activities, with safeguards in place to limit the inappropriate use and sharing of patient data. The HIPAA Privacy Rule takes critical steps in that direction to require that privacy and security be built in to the policies and practices of health care providers, plans, and others involved in health care. Despite the law's clear purpose and scope, a lack of widespread and consistent public education, training, and technical assistance has given rise to a number of persistent and destructive myths. The following are some common myths regarding the Privacy Rule and the facts about what the law actually says.

Myth #1: Health care providers can share personal health information with employers.

FACT: The Privacy Rule absolutely prohibits health care providers and plans from disclosing personal health information to employers without a patient's explicit, written authorization. A valid authorization under the law must include a description of the information to be shared, the name of the person allowed to use or disclose the information, an expiration date, and the signature of the individual. The Privacy Rule also covers self-insured employers when they are acting in their capacity as a health plan. These employers must construct an organizational firewall, so that the health care information they gather can only be used for health care related functions, and plan administrators are prohibited from sharing that information with other employees. However, some employers do collect health information independently, such as through workforce surveys. In this scenario, employers are not acting as health plans, and therefore are not covered by the law. §§164.508(a)(1), 164.504(a)

Myth #2: One doctor's office cannot send medical records of a patient to another doctor's office without that patient's consent.

FACT: No consent is necessary for one doctor's office to transfer a patient's medical records to another doctor's office for treatment purposes. The Privacy Regulation specifically states that a covered entity "is permitted to use or disclose protected health information" for "treatment, payment, or health care operations," without patient consent. As HHS explains, "treatment" includes "consultation between health care providers regarding a patient and referral of a patient by one provider to another." HHS states that providing health records to another health care provider for treatment purposes "can be done by fax or other means." §§164.502(a)(1)(ii), 164.506(a), <http://www.hhs.gov/ocr/privacysummary.pdf> (page 5), <http://www.hhs.gov/ocr/hipaa/> (FAQ section, page 1, questions 6 & 12).

Myth #3: The HIPAA Privacy Regulation prohibits or discourages doctor/patient emails.

FACT: The Privacy Rule allows providers to use alternative means of communication, such as email, with appropriate safeguards. Doctors and other healthcare providers may continue to communicate with patients via email. Both the HIPAA Privacy and Security Regulations require providers to use reasonable and appropriate safeguards to “ensure the confidentiality, integrity, and availability” of any health information transmitted electronically, and to “protect against any reasonably anticipated threats” to the security of such information. Therefore, a covered entity is free to continue using email to communicate with patients, but should be sure that adequate safeguards, such as encryption, are used. §§ 164.522(b)(1)(i), 164.306(a)(1)-(2), (d)(3)(i)-(ii), 164.312(e)(2)(ii).

Myth #4: A hospital is prohibited from sharing information with the patient’s family without the patient’s express consent.

FACT: Under the Privacy Rule, a health care provider may “disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual,” the medical information directly relevant to such person’s involvement with the patient’s care or payment related to the patient’s care. Uses and disclosures “for involvement in the individual’s care and notification purposes” are clearly permitted. The Rule states that if the patient is present, the health care provider may disclose medical information to such people if the patient does not object. If the patient is unable to agree or object to disclosure because of incapacity or an emergency circumstance, the covered entity may determine whether the disclosure is in the best interests of the patient. The professional judgment of the health care provider should inform any decision regarding disclosure of protected health information to a family member or friend who is involved in the patient’s care, as these disclosures are permitted, but not mandatory. If a hospital or other health care provider refuses to provide any relevant medical information to family members, it is again, the hospital policy, and not required by the Regulation. § 164.510(b)

Myth #5: A patient’s family member can no longer pick up prescriptions for the patient.

FACT: Under the Regulation, a family member or other individual may act on the patient’s behalf “to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.” The Regulation permits the health care provider to reasonably infer that doing so is in the patient’s best interest and in accordance with professional judgment and common practice. HHS specifically explains that the Rule “allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient.” Similarly, HHS issued guidance and a press release on July 6, 2001 that explicitly stated that “the rule allows a friend or relative to pick up a patient’s prescription at the pharmacy.” Therefore if pharmacies prohibit this common practice, it is their own policy, not one mandated by the HIPAA Privacy Regulation. § 164.510(b)(3), <http://www.hhs.gov/ocr/privacysummary.pdf> (page 6).

Myth #6: The Privacy Regulation mandates new disclosures of patient information.

FACT: As HHS states, disclosure is mandated in only two situations: to the individual patient upon request, or to the Secretary of the Department of Health and Human Services for use in oversight investigations. Disclosure is permitted, not mandated, for other uses under certain

limits and standards, such as to carry out treatment, payment, or health care operations, or under other applicable laws. Disclosure of protected health information has always been permitted for purposes such as national security, public health monitoring, and law enforcement, as well as many others. The Privacy Rule requires that patients be informed, through the notice of privacy practices, of these uses and disclosures. Nearly all of these uses and disclosures are permissive, so health care plans and providers may choose not to use or disclose medical information. §§ 164.502, 164.508, 164.512, 164.520, <http://www.hhs.gov/ocr/privacysummary.pdf> (pages 4-11).

Myth #7: A patient cannot be listed in a hospital's directory without the patient's consent and the hospital is prohibited from sharing a patient's directory information with the public.

FACT: The Privacy Rule permits hospitals to continue the practice of providing directory information to the public unless the patient has specifically chosen to opt out. The Regulation states that a health care provider, such as a hospital, may maintain a directory that includes the patient's name, location in the facility, and condition in general terms, and disclose such information to people who ask for the patient by name. The patient must be informed in advance of the use and disclosure and have the opportunity to opt out of having his or her information included in the directory. Emergency situations are specifically provided for in the Regulation, so if the patient is comatose, or otherwise unable to opt out due to an emergency, the hospital is permitted to disclose directory information if the disclosure is consistent with the patient's past known expressed preference and the provider determines disclosure is in the individual's best interest. The provider must provide the patient with an opportunity to object, "when it becomes practicable to do so." Any more restricted uses of directory information, such as requiring patients to ask to be listed in, or opt into, the directory, are either the hospital's own policy or confusion about the Privacy Regulation. §164.510(a), <http://www.hhs.gov/ocr/privacysummary.pdf> (page 6), <http://www.hhs.gov/ocr/hipaa/> (FAQ section, page 2, question 37).

Myth #8: The HIPAA Privacy Regulation imposes so many administrative requirements on covered entities that the costs of implementation are prohibitive.

FACT: The White House issued a report in March 2002 estimating the costs of implementing privacy over ten years at approximately \$18 billion and estimating the savings incurred from putting the transaction standards in place over ten years at approximately \$29.9 billion, thus saving the health care industry approximately \$12 billion overall. Further, there will be additional savings in the long term because patients will have more faith in the health care system, so they will be less likely to withhold vital information from their doctors, and will more readily seek care.

Myth # 9: Patients can sue health care providers for not complying with the HIPAA Privacy Regulation.

FACT: The HIPAA Privacy Regulation does not give people the right to sue. Even if a person is the victim of an egregious violation of the HIPAA Privacy Rule, the law does not give people the

right to sue. Instead, individuals must file a written complaint with the Secretary of Health and Human Services via the Office for Civil Rights. It is then within the Secretary's discretion to investigate the complaint. HHS may impose civil penalties ranging from \$100 to \$25,000, and criminal sanctions ranging from \$50,000 to \$250,000, with corresponding prison terms, may be enforced by the Department of Justice. However, since the law went into effect, HHS has focused on a complaint-driven process that relies on voluntary compliance with the law. So far, not one civil monetary penalty has been issued. §§ 160.306, 160.312 (a)(1), 160.304(b), 42 U.S.C § 1320 et seq., <http://www.hhs.gov./news/facts/privacy.html>.

Myth #10: Patients' medical records can no longer be used for marketing.

FACT: Use or disclosure of medical information is explicitly permitted for certain health related marketing under the HIPAA Privacy Rule. For example, communication about a plan's health related products or alternative treatments and services is not considered marketing for the purposes of the Rule—even if the health care provider is paid to encourage the patient to use the product or service. The 2000 version of the Privacy Rule required that patients be notified if the health care provider was paid to communicate about a health related product, be given the opportunity to opt out of future communications, and be informed of the identity of the source of the communication. The Bush Administration eliminated these safeguards from the Regulation. §§164.508(a)(3), 164.50, <http://www.hhs.gov/news/press/2002pres/20020809.html>.

Myth #11: If a patient refuses to sign an acknowledgment stating that she received the health care provider's notice of privacy practices, the health care provider can, or must, refuse to provide services.

FACT: The HIPAA Privacy Rule grants the patient a 'right to notice' of privacy practices for protected health information, and requires that providers make a "good faith effort" to get patients to acknowledge they have received the notice. The law does not grant health care providers the right to refuse to treat people who do not sign the acknowledgement, nor does it subject the provider to liability if a good faith effort was made. A health care provider or health plan "must provide a notice that is written in plain language" that informs the patient of "the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information." 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, to provide a copy of the notice to the patient upon request, to post a copy of the notice in a prominent location, and to "make a good faith effort to obtain a written acknowledgment of receipt of the notice" except in emergency situations. The acknowledgment of the receipt of notice of the privacy practices is not a consent for treatment. It is not an authorization for the release of medical records. A patient's signature acknowledging receipt of the notice, or her refusal, does not create or eliminate any rights, so it should not be the basis for providing or refusing treatment. § 164.520(b)(1), (a)(1), (c)(2)(i)-(iii)

Myth #12: The HIPAA Privacy Rule imposes many new restrictions on hospitals' fundraising efforts so that fundraising becomes almost impossible.

FACT: According to the Rule, a hospital may use, or disclose to its “business associate” or an institutionally related foundation, demographic information and the dates of health care provided to an individual “for the purpose of raising funds for its own benefit, without an authorization [from the patient].” Such use or disclosure is not permitted unless disclosed in the notice of privacy practices. Any fundraising materials that the covered entity sends to an individual must include a description of how the individual may opt out of future fundraising communications. Therefore, the Rule does not hinder fundraising in the first instance, and if a covered entity wants to target specific patients it must include this information in its notice of privacy practices. Hospitals must also make reasonable efforts to ensure that those who decide to opt out of receiving future fundraising communications do not continue to receive such communications. §§ 164.514(f)(1)-(2), 164.520(b)(1)(iii)(B).

Myth #13: The press can no longer access vital public information from hospitals about accident or crime victims.

FACT: HIPAA allows hospitals to continue to make public (including to the press) certain patient directory information - including the patient’s location in the facility and condition in general terms - unless the patient has specifically opted out of having such information publicly available. Thus, if a patient has not opted out of being listed in a hospital directory, and a reporter knows the name of an accident or crime victim, the reporter can request directory information from a hospital, including the condition of the patient. HIPAA does prohibit the hospital from releasing anything more than directory information, without the patient’s authorization. This HIPAA provision, however, is not a change from most existing state laws, which protect the confidentiality of patient information to varying degrees. Further, the HIPAA Privacy Rule does not directly cover the media, so once a reporter obtains patient information, from any source, he or she is not restricted by HIPAA in how the information is used or disclosed.

For more information, see the Health Privacy Project’s web site at www.healthprivacy.org. Or contact HPP’s Policy Analyst, at 202-721-5614 (info@healthprivacy.org).