

Chapter 16

Federal Health Information Privacy Requirements

Karen S. Rieger, JD

Federal Health Information Privacy Regulations
State Health Information Privacy Laws

Conclusion

The public's assurance of privacy in health care information must be preserved so that patients remain willing to communicate sensitive personal information to their health care providers. Failure to address privacy concerns undermines public confidence in the health care system. Protection of confidential medical information may encourage individuals to seek treatment and seek it earlier. Maintaining confidentiality of health information bolsters the health care system while reducing liability risks to the providers charged with protecting the private information they receive. Federal law and state laws have requirements regarding access to, and protection of, health care information, as summarized below.

FEDERAL HEALTH INFORMATION PRIVACY REGULATIONS

On December 28, 2002, the Department of Health and Human Services released the final version of the federal health information privacy regulations, which were implemented in conjunction with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191.¹ Amendments to the privacy regulations were published in the *Federal Register* on August 14, 2002.² These regulations are located in the Code of Federal Regulations at 45 C.F.R. Parts 160 and 164. The regulations are referenced in this chapter as the HIPAA Privacy Regulations. In most cases, compliance with the HIPAA Privacy Regulations was required on or before April 14, 2003.

The purposes of the HIPAA Privacy Regulations are to (1) provide consumers access to their health information and control inappropriate uses of their information; (2) improve the quality of health care by restoring trust in consumers; and (3) improve the efficiency and effectiveness of health care delivery by creating a national framework for the use and disclosure of sensitive health care information.³

Covered Entities

The HIPAA Privacy Regulations apply to health information created or maintained by "Covered Entities," which are defined to include (1) health plans, (2) health care

clearinghouses, and (3) health care providers who transmit any health information in electronic form in connection with a transaction covered by the HIPAA Privacy Regulations.⁴ The HIPAA Privacy Regulations protect individually identifiable health information that is created or received by a health care provider, health plan, employer, or health care clearinghouse and that relates to the past, present, or future physical or mental health of a person, the provision of health care to a person, and/or the payment for health care.⁵ Such protected health information is referenced in this chapter as "PHI."

Use and Disclosure for Treatment, Payment, and Health Care Operations

Under the HIPAA Privacy Regulations, a Covered Entity may use or disclose a patient's PHI without obtaining patient consent or an authorization for purposes of treatment, payment, and health care operations.⁶ "Treatment" under the regulations includes the provision, coordination, or management of health care and related services by one or more health care providers, including coordination of care between a provider and 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.⁷ The use for "payment" purposes includes a broad range of activities, including determination of insurance coverage and/or eligibility for coverage; billing and collection activities; and utilization review activities.⁸ "Health care operations" is defined in the HIPAA Privacy Regulations to include such things as business and financial planning; peer review and quality assurance activities; conducting or arranging for accounting, legal, and other professional services; and business management and administrative activities.⁹

Written Authorization Requirements

For uses and disclosures of PHI *other than* for treatment, payment, and health care operations, the Covered Entity must obtain the patient's written authorization unless otherwise permitted or required by law.¹⁰ The HIPAA Privacy Regulations set forth specific requirements for this written

160 Federal Health Information Privacy Requirements

authorization form. In particular, the form must be written in plain language and is required to include the following:

- Who can disclose the PHI subject to the authorization.
- The exact information authorized to be disclosed.
- The purpose of the disclosure.
- The right of the patient to revoke the authorization, and the effect of a revocation.
- The name or class of persons to whom the covered entity is authorized to release the PHI.
- An expiration date or event.
- Whether the Covered Entity will receive any compensation/remuneration in connection with the PHI authorized to be released.
- A statement that the PHI authorized for disclosure may be redisclosed by the recipient and not protected.
- The signature of the patient or his or her legally recognized personal representative.¹¹

In addition to the elements of an authorization required under the HIPAA Privacy Regulations, applicable state law may require an authorization to include additional information.¹²

Notice of Privacy Practices

The HIPAA Privacy Regulations also require health care providers, on the first encounter with the patient following August 14, 2003, to provide patients with a written notice of the provider's privacy policies and to make a good faith effort to obtain written acknowledgment of the patient's receipt of the notice. A health plan was required to provide this notice by April 14, 2003, unless it qualifies as a small health plan, which have another year to comply.¹³

If a Covered Entity is not able to obtain a written acknowledgment of the patient's receipt of the notice, it should document in its records the reasons such acknowledgment could not be obtained.¹⁴ The notice of privacy practices is required to include a number of specific disclosures.¹⁵

Business Associate Requirements

Although the HIPAA Privacy Regulations cover only the Covered Entities mentioned above, the regulations expand protections by requiring that Covered Entities obtain written assurances from their "business associates" that the business associate will appropriately safeguard the individual's PHI.¹⁶ Business associates are individuals or entities, other than members of the Covered Entity's workforce, that receive, create, or have access to PHI and perform a function or service on behalf of the Covered Entity.¹⁷ The business associate agreement also must include provisions such as the following: restrictions on how the business associate may use or disclose the PHI; a promise to protect the information; an obligation to return or destroy the information at the end of the contract; and assurances to make the information available to the Covered Entity for compliance purposes.¹⁸ The commentary to the August 14, 2002 amendments to the HIPAA Privacy Regulations contains some sample language for business associate agreements.¹⁹

However, Covered Entities should consult with their legal counsel before using such language, to be certain that the agreements are drafted in a manner that complies with applicable state law.

Certain Permitted/Required Uses and Disclosures

The general rule under the HIPAA Privacy Regulations is that a Covered Entity may not use or disclose an individual's PHI without the individual's written authorization (1) except for treatment, payment or health care operations, or (2) unless otherwise permitted or required by the HIPAA Privacy Regulations or other laws or regulations. However, unrestricted access and/or disclosure of PHI may be necessary for certain purposes such as protecting the public health, reducing health care fraud, and improving the quality of treatment of patients. In these instances, obtaining an authorization may hinder a health care provider's ability to adequately protect and promote public health. Therefore, in certain limited circumstances, a health care provider may disclose PHI without the patient's consent, authorization, or providing the patient the opportunity to agree or object. This includes but is not limited to the following:

- Reporting abuse or neglect of children and vulnerable adults.
- Reporting criminally inflicted injuries.
- Certain limited disclosures to law enforcement officials.
- Disclosures to appropriate health authorities conducting public health surveillance, public health investigations, public health interventions, and regulatory oversight.
- Disclosures for purposes of the Medicaid program.
- Reports of certain deaths to the medical examiner.
- Disclosures to funeral directors and for cadaveric organ, eye, or tissue donations.
- Disclosures under workers' compensation laws.²⁰

Disclosures in Facility Directories

In addition to the exceptions above, a Covered Entity may include certain patient information in a facility directory (i.e., the patient's name, location within the facility, and one-word condition, such as fair, critical, serious, or death), disclose it to members of the clergy, or disclose it to family or close friends of the patient who ask for the patient by name without patient authorization. The Covered Entity must give the patient the opportunity to object or agree to these disclosures. The objection may be oral or in writing.²¹

Research Requirements

As noted above, a health care provider may use a patient's PHI in the course of treatment, payment, and health care operations without obtaining an authorization. However, because most research activities fall outside of these areas, specific patient authorization is generally necessary for use or disclosure of PHI for research purposes unless an exception applies. The HIPAA Privacy Regulations do permit providers to use or disclose research information using data

that has been stripped of its identifiers, known as “de-identified health information.” De-identified health information is health information that does not identify the patient and in which there is no reasonable basis to believe that the health information can be used to identify the patient. Because de-identified health information has been stripped of all identifiers, it is not subject to authorization requirements.²²

Limited Data Set Use

A “limited data set” is an additional disclosure method applicable to research. A limited data set is PHI that does not directly identify the patient, but which contains certain potentially identifying information. A limited data set may be used or disclosed by a provider without patient consent or authorization only for the purposes of research, public health, or health care operations, and is subject to certain restrictions. Limited data sets have the same identifiers removed as de-identified data sets with three exceptions. Limited data sets may include identifiers such as birth date, dates of hospital admissions and discharges, and an individual’s residence by city, county, state, and five-digit zip code. Recipients of PHI contained in limited data sets must enter into a data use agreement with the provider before receiving the limited data set. Certain other limited exceptions permit disclosure of a patient’s PHI without consent or authorization in certain limited circumstances.²³

Specific Patient Rights

In addition to placing restrictions on a Covered Entity’s ability to use or disclose PHI, the HIPAA Privacy Regulations also provide patients with certain rights regarding their PHI. These include the following.

Access to PHI

Generally, a patient has the right to access, inspect, and obtain a copy of his or her PHI upon request. This does not include psychotherapy notes, records compiled by a Covered Entity in reasonable anticipation of, or for use in, a civil, criminal, or administrative proceeding, or information subject to law that prohibits access to such information. There also are some limited circumstances under which a patient or his or her personal representative can be denied access to the patient’s PHI if a licensed health care professional believes such access would endanger the patient or another person.²⁴

Amendment of PHI

A patient has the right to request the Covered Entity to amend the patient’s PHI for as long as the information is maintained by the Covered Entity. The Covered Entity may deny the request for an amendment if the patient asks to amend information that: (1) was not created by the Covered Entity, unless the person or entity that created the information is no longer available to make the amendment; (2) is not part of the medical health information kept by the Covered Entity; or (3) is not part of the information

which a patient is permitted to inspect and copy by law. Further, a Covered Entity may deny a request for amendment if it believes the information is accurate and complete. If the Covered Entity declines to make a requested amendment to a patient’s PHI, the patient is permitted to submit a written statement regarding the amendment that was requested. This statement must be included with the patient’s medical record and released as part of the record.²⁵

Accounting of Disclosures

Patients have a right to request a list of certain disclosures the Covered Entity has made of their PHI. This right does not include disclosures made for treatment, payment, and health care operations; disclosures for certain law enforcement activities; disclosures of directory information and/or disclosures to family members or friends involved in the patient’s care; disclosures pursuant to an authorization; or disclosures to the individuals themselves.²⁶

Restrictions

A Covered Entity must permit a patient to request certain restrictions on the use and disclosure of his or her PHI. The Covered Entity is not obligated to agree to such requested restrictions. However, if it does agree to a restriction, it may not use or disclose PHI in violation of the restriction.²⁷

Communications by Alternative Means

A Covered Entity must permit patients to request to receive communication of PHI by alternative means or at alternative locations. The Covered Entity must accommodate any reasonable requests and may not require an explanation.

Minimum Necessary Rule

A key requirement of the HIPAA Privacy Regulations is that a Covered Entity must make reasonable efforts to limit protected health information used and/or disclosed to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.²⁸ For example, if a consulting physician needs to review only a specific portion of the patient’s medical record, only that portion should be disclosed. Further, members of a Covered Entity’s workforce should only access and use the portions of a patient’s PHI that such person needs to perform his or her job functions. The Department of Health and Human Services has indicated that the use of reasonable safeguards will be acceptable to meet this requirement. For example, patient files should be maintained in locked file cabinets when they are not needed for treatment, payment, or health care operational purposes, and should not be left unattended on desks and in other locations where the patient’s PHI could be inadvertently seen. On the other hand, the regulators have made clear that the “reasonable necessary” requirement will still permit the use of patient sign-in sheets, surgery scheduling boards, and other common practices of health care professionals that might result in the disclosure of a minimal amount of PHI.²⁹

162 Federal Health Information Privacy Requirements

Penalties for Noncompliance

A number of penalties may be imposed on Covered Entities that violate the HIPAA Privacy Regulations. In particular, a civil penalty of \$100 per violation, not to exceed \$25,000 per person per calendar year, may be imposed. In addition, the following criminal penalties can be imposed for egregious violations:

- Up to \$50,000 and/or 1 year in prison for knowingly misusing PHI.
- Up to \$100,000 and/or 5 years in prison for using PHI under false pretenses.
- Up to \$250,000 and/or 10 years in prison for inappropriately using PHI for “commercial advantage.”³⁰

The HIPAA Privacy Regulations do not give an individual patient the right to sue a Covered Entity for noncompliance. Thus, only the government may seek to enforce these regulations.

STATE HEALTH INFORMATION PRIVACY LAWS

The HIPAA Privacy Regulations were adopted, in part, to create a uniform, national system for the use and disclosure of medical records and other PHI. These regulations provide that they will preempt, or take precedence over, any state laws that are contrary to the provisions of the HIPAA Privacy Regulations. A state law is considered contrary if (1) it is not possible to comply with both, or (2) the state law is an obstacle to accomplishing and executing the purposes and objectives of the HIPAA Privacy Regulations.³¹ However, there are some situations, or exceptions, in which a state law will not be preempted, and will continue to apply. The exceptions applicable to health care providers are described below.

First, state laws that provide for the reporting of disease or injury, child abuse, birth and death statistics, and/or the conduct of public surveillance, investigation, or intervention in order to promote public health, will not be preempted by the HIPAA Privacy Regulations.

Second, the Secretary of the Department of Health and Human Services, upon a written request from a state governor, may request an exception for a specific state law in order to (1) prevent fraud and abuse; (2) ensure appropriate state regulation of insurance and health plans; (3) provide for state reporting on health care delivery or costs; or (4) to serve a compelling need related to public health, safety, welfare, etc. To date, no such exception has been requested by any governor.

Third, and perhaps most importantly, the HIPAA Privacy Regulations do not preempt state laws that are more “stringent” than the requirements of the HIPAA Privacy Regulations. A state law is more stringent if (1) it is more restrictive on use and disclosure of PHI; (2) it permits greater rights of access or amendment by a patient to his or her PHI; (3) it provides the patient more information about the use, disclosure, rights, and/or remedies relating to his or her PHI; (4) in connection with a state law dealing with

the required form, substance, or need for express legal permission to release, the state law narrows the scope or duration of permitted releases of the patient’s PHI, increases privacy protections, or reduces coercive effects regarding release; (5) it requires retention or reporting of more detailed information and/or for a longer duration; and (6) it provides greater privacy protection to the patient regarding his or her PHI.

Many states have physician/patient privilege laws that, subject to a number of exceptions, allow the patient to prevent the disclosure of the patient’s health information without the patient’s specific consent.³² Courts have recognized a health care provider’s obligation to invoke a privilege on the patient’s behalf, to the extent protected information is requested from the provider.³³ A physician/patient privilege law generally permits a patient to prevent the disclosure of his or her health information that was disclosed to a health care provider for purposes of diagnosis and/or treatment. Courts have not recognized the privilege in connection with disclosures made for other purposes. For example, in the case of *Tarrant County Hospital District v. Hughes*,³⁴ a hospital was required to release the names of blood donors whose blood was infused into a patient who contracted AIDS. The court found that this information was not provided for diagnosis and/or treatment of the blood donors.

As noted above, the HIPAA Privacy Regulations do not require patient consent in order for the patient’s physician or other health care provider to release and use the patient’s PHI for treatment, payment, and/or health care operations. However, because state physician/patient privilege laws may provide greater protection for a patient’s PHI when the patient has not waived the privilege, such laws will not be preempted by the HIPAA Privacy Regulations. In addition to the physician/patient privilege statute, many states have other professional privilege laws that also provide more protection for a patient’s PHI, and will not be preempted. These include patient/social worker privilege laws; patient/psychologist privilege laws; patient/licensed professional counselor privilege laws; and licensed marital and family therapist privilege laws.

Further, many states have laws that contain some very restrictive requirements regarding the use and disclosure of a patient’s PHI that may contain communicable disease information,³⁵ and records containing mental health information and/or substance abuse information.³⁶

CONCLUSION

It is important for all health care providers to understand their obligations under both the HIPAA Privacy Regulations and any applicable state health information privacy laws and regulations. This chapter should be viewed as a starting point in identifying key health information privacy requirements, and directing such professionals to more detailed information regarding these legal issues. A health care provider should consult with any attorney licensed in his or her state to obtain specific advice regarding the health information privacy requirements applicable in that particular state.

Endnotes

1. 65 Federal Register 82462.
2. 67 Federal Register 53182.
3. *Id.*
4. 45 C.F.R. §160.103.
5. 45 C.F.R. §160.103.
6. Because of ambiguities regarding consent requirements imposed by a state, however, it may nonetheless be necessary in some instances for a Covered Entity to obtain patient consent.
7. 45 C.F.R. §164.501.
8. 45 C.F.R. §164.501.
9. 45 C.F.R. §164.501.
10. For example, an individual's authorization is required for fundraising activities, except for limited activities involving only demographic information and date of service, and for marketing activities, except for certain face-to-face encounters and promotional gifts of nominal value.
11. 45 C.F.R. §164.508.
12. For example, Oklahoma law requires that the following language be included in order for an authorization to be valid: "The information authorized for release may include records which may indicate the presence of a communicable or venereal disease which may include, but are not limited to, diseases such as hepatitis, syphilis, gonorrhea and the human immunodeficiency virus, also known as acquired immune deficiency syndrome (AIDS)."
13. 45 C.F.R. §164.520.
14. 45 C.F.R. §164.520(c)(2)(ii).
15. 45 C.F.R. §164.520.
16. 45 C.F.R. §164.504(e).
17. 45 C.F.R. §160.103.
18. 45 C.F.R. §164.504(e).
19. 67 Federal Register 53264.
20. 45 C.F.R. §164.512.
21. 45 C.F.R. §164.510.
22. 45 C.F.R. §164.514.
23. 45 C.F.R. §164.514.
24. 45 C.F.R. §164.524.
25. 45 C.F.R. §164.526.
26. 45 C.F.R. §164.528.
27. 45 C.F.R. §164.522(a).
28. 45 C.F.R. §164.502.
29. *See, e.g.*, OCR HIPAA Privacy Guidance, December 3, 2002.
30. 42 U.S.C. §1320d-5, 42 U.S.C. §1320d-6.
31. 45 C.F.R. §160.201 *et seq.*
32. *See, e.g.*, 12 Okla. Stat. §2503.
33. *Hospital Corporation of America v. Superior Court of Pima County*, 755 P. 2d 1198 (Ariz. App. 1988); *Parkson v. Central Du Page Hospital*, 435 N.E. 2d 140 (Ill. App. 1982).
34. 734 S.W. 2d 675 (Tex. App. 1987).
35. *See, e.g.*, 63 Okla. Stat. §1-502.2.
36. *See, e.g.*, 43 A Okla. Stat. §1-109.

