Why the HIPAA Privacy Rules Are Important for Physicians to Know

Ignore these at your own risk.

BY TIMOTHY E. PATERICK, MD, JD

The Health Insurance Portability and Accountability Act (HIPAA) is important for physicians to review so they can understand its impact on their daily medical practice. The HIPAA Privacy Rule is complicated, highly detailed, and broad in its administrative bandwidth. Violation of any of HIPAA's enumerated mandates by physicians has the potential for loss of medical license, civil and criminal fines, and imprisonment.

This article explores the following features of the HIPAA Privacy Rule:

- What HIPAA mandates;
- What entities the Privacy Rule applies to;
- The definition of a personal representative;
- The definition and meaning of personal health information (PHI);
- The definition of de-identified PHI;
- How mental health records are handled;
- The uses and disclosures of PHI;
- The difference between authorization and consent for use and disclosure of PHI;
- The circumstances under which HIPAA allows or requires the disclosure of PHI;
- The minimum necessary standard regarding PHI;
- The definition of a notice of privacy practices;
- The rights of patients under the HIPAA Privacy Rule; and
- The Privacy Rule administrative requirements.

Third parties, called business associates (BAs), that have access to patient information also must comply with HIPAA.

Despite the lengthy, detailed, and granular aspects of HIPAA, this is a marathon that every physician should run.

What Is the HIPAA Privacy Rule?

The HIPAA Privacy Rule requires physicians to implement policies and procedures that protect the privacy of patients' PHI and regulates how physicians use and disclose PHI with and without patient authorization. The Privacy Rule was intended to provide patients with rights over their health information, such as the right to see their health records, acquire a personal copy of their PHI, and request amendments of errors in the PHI. The Privacy Rule is the first comprehensive federal protection of the privacy of health information, creating a national standard to protect an individual's PHI.

What Was the HIPAA Privacy Rule Meant to Do?

The Privacy Rule, succinctly stated, was meant to give patients more control over their PHI, set boundaries on the use and release of PHI, establish safeguards that physicians must apply with to protect PHI, hold violators of HIPAA accountable, and strike a balance when there is a public need for disclosure of PHI.

To What Entities Does the Privacy Rule Apply?

HIPAA applies to what are called covered entities (CEs). This category includes, but is not limited to, physicians who perform standard electronic transactions, health plans, and healthcare clearinghouses. Third parties, called business associates (BAs), that have access to patient information also must comply with HIPAA. The task of identifying who is a CE and BA can be daunting. The reader needs to be aware of what is classified as a CE and a BA and to know one's accountability and vulnerability to HIPAA rules. A health plan is an individual or group plan that pays for medical care.

The law outlines various organizations and government programs as

Continued on page 114

HIPAA (from page 113)

health plans. These include insurance companies, CMS, the Children's Health Insurance Program (CHIPS), the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), and prescription drug programs. A healthcare clearinghouse is a public or private entity that must comply with HIPAA, such as a billing service, a community health management information system, or a community health information system. Healthcare providers are individuals or organizations that bill or are paid for medical services as part of their business.

Affiliated CEs are legally separate entities that are under common ownership. An example is an integrated delivery network that includes hospitals, medical groups, and long–term care facilities.

A business associate is a person or entity that is not part of the CE's staff, but performs activities on behalf of the CE that include the use or disclosure of PHI. Activities performed by a BA might include, but are not limited to, claims processing or administration; data analysis (processing or administration); utilization review; quality assurance; benefits management; and practice management.

Once a CE recognizes it has a business relationship that meets the definition of a BA, the CE is responsible for guaranteeing that the BA complies with HIPAA rules. This is accomplished by means of a covenant between the CE and the BA. This contract is known as a business associate agreement (BAA). The BAA is a written contract between the parties that specifies each party's duties with regard to the PHI.

There are exceptions to the BA standard. HIPAA does not demand CEs to have a BAA in place before PHI can be disclosed in the following situations:

- Disclosure of PHI by a CE to a physician for treatment. For example, a hospital does not need a BAA with a specialist to whom it refers a patient.
- Disclosure of PHI by a physician to a medical laboratory to treat a patient.

There are many more exceptions, and navigating the relationships can be intimidating. When uncertainty exists, obtain legal advice as to the nature of the relationship.

The key reason HIPAA exists is to make CEs take measures to keep PHI private and confidential, and to identify and police the reasons that PHI can be used, shared, or disclosed.

What Is a Personal Representative?

Patients have the right to select a chosen individual to act on their behalf regarding their PHI. These personal representatives (PRs) have the same rights as the patient concerning the patient's PHI. The PR may have broad authority to act on the patient's behalf, or the authority may be limited at the patient's request. The CE and BA must observe the limits set by the patient. The CE and BA should review state law to identify whether there are regulations regarding the authority of PRs. For example, HIPAA defers to state laws that expressly speak to a parent's right to access children's PHI. If a CE has reasons to believe a patient is the victim of domestic violence, or neglect by the PR, the CE can legally choose not to recognize the PR.

What Is Personal Health Information (PHI)?

Personal health information is defined as individually identifiable health information held or transmitted by a CE or BA on paper, electronically, or orally, that identifies the patient and relates a patient's present or past physical or mental health condition. Additionally, PHI may be identified through present or past billing statements or payments for treatment.

Types of PHI include identifiers of the individual associated with health information, such as, but not limited to, name, address(es), telephone number, fax number, email, date of birth, date of death, hospital admission and discharge, driver's license number, and many other identifiers. Any of these data could be used to identify someone and link that person to his or her PHI.

What Is De-Identified Personal Health Information?

De-identified patient data is information that cannot be used to connect an individual to PHI. HIPAA does not apply to de-identified health information. It is a valuable asset to the healthcare community because it can be used to improve medical care, estimate the costs of medical care, and support public health initiatives.

What Are Disclosures of Personal Health Information?

HIPAA protects an individual's right to keep PHI private and confidential. However, there are valid reasons that physicians may need to use and share PHI, such as communicating with insurance companies for payment and sharing PHI with other physicians for patient medical care.

The key reason HIPAA exists is to make CEs take measures to keep PHI private and confidential, and to identify and police the reasons that PHI can be used, shared, or disclosed. There is a dynamic equilibrium between privacy/confidentiality and optimal information for quality medical care.

What Is the Difference Between Authorization and Consent?

Patients may give written authorization or consent for use and disclosure of their PHI. The Privacy Rule does not compel CEs to obtain patient authorization for medical treatment, payment, and healthcare operations. Patient authorization is an agreement that allows CEs to use and disclose PHI for purposes other than healthcare operations. CEs need authorization before using or disclosing PHI for any reason that is not

Continued on page 116

HIPAA (from page 114)

allowed under the Privacy Rule. Relying on a patient's consent when authorization is required is an unauthorized use of PHI. An important distinction is that consent does not equal authorization.

When Does HIPAA Allow or Require Disclosure of Personal Health Information?

HIPAA permits CEs to use their professional ethics and best judgment to share PHI without patient authorization in clearly defined situations. CE permitted disclosures include the following:

- Disclosure to the patient;
- Disclosure for medical treatment, payment, and healthcare operations;
- When patient is allowed to agree/reject use or disclosure;
- Use or disclosure for public benefit;
- Limited data set research; and
- Public health purposes.

CE required disclosures include:

- Patient request for PHI;
- Patient request for an accounting of disclosures;
- Disclosure to HHS for the purpose of compliance investigation, reviews, or an enforcement action; and
- Protection of the patient and the public.

The duty to inform the patient and public has its foundation in the 1974 California Supreme Court case Tarasoff v. the Regents of the University of California, 551 P2d 334 (Cal.1976), which established a duty for physicians to share warnings of a credible threat of violence. That duty was reaffirmed in the 2013 Office of Civil Rights letter,[1] which sought to balance patient privacy concerns with public health and safety.

What Is the Minimum Necessary Standard?

The Privacy Rule exists to guarantee that any PHI accessed by staff or disclosed to another CE or BA is done in a minimal manner that protects and safeguards confidentiality. This is known as the minimum necessary standard and is an essential protection. CEs are mandated to limit use or disclosure of PHI to the minimum necessary standard to accomplish the intended purpose. In light of the minimum necessary standard, CEs determine which staff need access to PHI based upon staff responsibilities.

Refusal to sign the NPP does not alter the CE's need to comply with the Privacy Rule.

There are exceptions to the minimum necessary standard, including:

- Disclosure to a physician for medical treatment purposes;
- Authorization of use/disclosure by the patient;
- Use/disclosure required for HIPAA compliance;
- Required by HHS for enforcement purposes; and
- Required by state laws.

What Is a Notice of Privacy?

A notice of privacy practices (NPP) is a statement by the CE that describes how it will disclose PHI and the procedure the CE has executed to keep PHI confidential. It also explains how patients can access their information and exercise this right under HIPAA. CEs are required to write an NPP in plain and understandable language and make it available to all patients.

A CE that has a direct doctor–patient relationship must provide a copy of the NPP on the patient's first visit and make a good faith effort to obtain written acknowledgement of receipt.

Additionally, the CE should make its NPP available to anyone who requests it and post it in full view at the physical location and on its website. The CE cannot compel the patient to sign the NPP, and it cannot refuse treatment if the patient refuses to sign the NPP. Refusal to sign the NPP does not alter the CE's need to comply with the Privacy Rule. Staff should attempt to document why the patient refuses to sign the NPP.

What Are the Rights of the Patient under The HIPAA Privacy Rule?

HIPAA provides patients with a general right to access, inspect, and acquire a copy of their PHI for as long as a CE or BA maintains the information. Patients may request a summary or explanation of PHI and have the right to direct the CE to share a copy of this PHI with a PR. A CE must comply with the request within 30 days. The CE can obtain a 30-day extension with written notice to the patient stating the reasoning for the delay.

Patients have the right to specify how they would like the CE to communicate regarding their PHI and to request the CE to make amendments to the PHI. If the CE agrees to amend the PHI, it must make an addendum to the medical record and communicate the amendment to all individuals who rely on the patient's PHI. The CE must inform all parties involved, and those CEs and BAs must make the amendments.

The patient has a right to file a complaint if they believe the covered entity or business associate has committed a Privacy Rule violation.

Patients also have the right to request an accounting of disclosures. These requests can be made orally or in writing.

The CE should document the request on an authorization form. The accounting of disclosures must be kept with the PHI, along with the request for accounting and the name of the person who provided

Continued on page 117

HIPAA (from page 116)

the accounting. The CE must complete an accounting of disclosures within 60 days. A 30-day extension is possible if the CE provides a written statement explaining the delay and the expected date the accounting will be completed. The patient has a right to file a complaint if they believe the CE or BA has committed a Privacy Rule violation. The CE must develop and implement a procedure that patients can use to file such a complaint.

What Are the Privacy Rule Administrative Requirements?

The HIPAA Privacy Rule through its rulings requires CEs to develop a comprehensive blueprint to safeguard PHI and avoid barred uses and disclosures of PHI. Entities that do not develop and implement a comprehensive plan risk significant fines, costly curative measures, and reputational damages. The Privacy Rule's administrative requirements say there must be the following:

- A designated privacy official;
- A training program for privacy policies and procedures;
- Privacy rule guardrails and safeguards;
- A process for complaint filing;
- Sanctions for privacy violations;
- A mitigation plan;
- No retaliation or waiver of rights toward complainants;
- Policies and procedures for PHI protection; and
- Development of a management policy for PHI protection.

Conclusion

Physicians benefit from being educated and knowledgeable about the requirements of HIPAA that relate to PHI. The benefits include an understanding of how the Privacy Rule impacts their daily interaction and management of patients' medical care.

There is a dynamic balance in managing privacy and optimal medical care. Failure to understand these subtleties of the Privacy Rule and ensuing Privacy Rule violations can result in physician sanctions that affect their ability to practice medicine.

Transgression of any of the enumerated mandates of the Privacy Act by physicians has the potential for loss of medical license, civil and criminal fines, and imprisonment. **PM**

Reference

[1] Health Insurance Portability and Accountability Act of 1996. aspe.hhs.gov

Suggested Readings

HIPAA Security Rule: hhs.gov

HIPAA Privacy Rule: hhs.gov

HIPAA Compliance and Enforcement Rule: hhs.gov

Dr. Paterick is a cardiologist at Bay Care Clinic, Green Bay, Wisconsin; email: tpaterick@gmail.com.