PARTNERSHIP *for*
PUBLIC HEALTH LAW
Advancing Public Health Through Law

Federal Protection of Personal Health Information

Personal health information is critical to the public health activities of state and local government, including disease surveillance and disease investigation. However, important federal laws affect how you may gather and disseminate this information. Under the Health Insurance Portability and Accountability Act (HIPAA), the U.S. Department of Health and Human Services (DHHS) created **a set of national privacy standards for health information**, known as the Privacy Rule. DHHS also created a set of security standard to help protect health information in its electronic form, the Security Rule. The Security Rule was strengthened by the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH). In addition to these federal laws, it is important to be familiar with state privacy and security standards because some states provide greater protections than those required by the federal government.

Who is Covered by HIPAA?

HIPAA privacy regulations only apply to **covered entities**. To be considered a covered entity, your organization must fall into one of three categories: (1) **a health plan-** individual or group plans that provide or pay the cost of medical care; (2) **a health care clearinghouse-** billing services, re-pricing companies, community health information systems and other entities engaging in certain information processing; or (3) **a health care provider-** medical or health services (physicians, hospitals, clinics, dentists) that electronically **transmit certain health information**.[1] For example, a local health department clinic that files electronic claims for health care services with Medicare and Medicaid is a covered entity. In addition, **business associates,** entities that use protected health information to perform certain work on behalf of covered entities, are also required to abide by the provisions of HIPAA.[2]

An organization can designate itself as a hybrid entity if it provides covered and non-covered functions.[3] As a hybrid entity, the organization must separate its covered and non-covered functions for Privacy Rule and Security Rule purposes. For example, a health department may have a public health clinic that qualifies as a health care provider and an environmental health office. On its own, the environmental health office does not qualify as a covered entity. If the health department designates itself a hybrid entity, the environmental health office is not subject to Privacy Rule or Security Rule, even though the health clinic is covered.

To determine whether your organization is subject to HIPAA, you should consult with your counsel.

What Information is Protected?

HIPAA only protects information designated as **protected health information** (PHI). PHI includes individually identifiable information related to (1) past, present or future physical and mental health conditions; (2) provision of health care; and (3) payment for health care that identifies the individual or could reasonably be used to identify the individual.[4]

In addition, the Privacy Rule lists 18 personal identifiers, including names, telephone numbers, email addresses, social security numbers, medical record numbers and health plan beneficiary numbers.[5] If any of these personal identifiers are present with medical information, they will trigger HIPAA's privacy requirements.

It is important to note that the **Privacy Rule** applies to all forms of PHI—whether electronic, written or oral—of a covered entity.[6]

However, HIPAA **excludes** certain types of records from its definition of PHI, e.g., certain education records, employment records held by a covered entity in its role as an employer and records regarding a person who has been deceased for over 50 years.[7]

The privacy requirements of HIPAA also **do not apply** to de-identified health information—information that cannot be traced back to a certain individual easily. There are two ways to de-identify health information: (1) remove all of the 18 personal identifiers or (2) have a qualified expert formally determine that the information is de-identified.[8]

Disclosing Information

Generally, covered entities can only share PHI with the written authorization of the individual.[9] However, there are several instances when covered entities **can** disclose PHI without the individual's authorization. The primary situations are the broad categories of medical treatment, payment and health care operations. However, there are additional instances when covered entities can disclose PHI without authorization related to: public health; abuse, neglect or domestic violence; judicial and administrative proceedings; law enforcement; and research.[10]

The public health exemption is a broad provision that allows covered entities to provide PHI to **public health authorities** in an array of situations.[11] Public health authorities are any federal, state, tribal or local agencies responsible for the public's health under an official mandate.[12] Information can be given to these authorities without the authorization of the patient for the purpose of preventing or controlling disease, injury or disability.[13] This includes public health investigations and public health interventions. For example, a health care provider that is a covered entity can disclose PHI related to a communicable disease to the local health department to help with disease surveillance. The provider must record its disclosure because it may be required to provide the patient with an accounting of its disclosures in certain situations.[14]

There are strict guidelines to each of the permitted exceptions. Always consult with counsel when dealing with a HIPAA disclosure.

Even when the Privacy Rule permits use or disclosure of PHI, a covered entity must be careful of what information is disclosed. The Privacy Rule requires that a covered entity use, disclose or request **the minimum amount of PHI necessary to meet the intended purpose**.[15]

Security Measures

HIPAA's **Security Rule** requires a variety of protections to prevent unauthorized access to **electronic PHI**. Both covered entities and their business associates must comply with these requirements.[16] These protections are generally categorized as administrative, physical or technical safeguards.[17] Required **administrative safeguards** include policies and procedures related to risk analysis and management, information access and security awareness and training programs.[18] **Physical safeguards** include controlling facility access and implementing safeguards on workstations that access electronic PHI.[19] Finally, **technical safeguards** include encryption of PHI and user authentication procedures.[20]

In addition, HITECH created new security breach notification provisions applicable to covered entities and their business associates. Generally, a breach is the unauthorized acquisition, access, use or disclosure of protected health information that compromises the security or privacy of the protected health information.[21] A covered entity has a duty to inform the individual whose PHI has been compromised within 60 days and in writing.[22]

If there is insufficient or out of date contact information for more than 10 individuals affected by the security breach, additional requirements apply. The covered entity must post information about the breach on its website or through major publications and broadcast media and must designate a phone line for inquiries regarding the breach. If a security breach affects 500 or more individuals, the covered entity must notify major media outlets and DHHS.[23] In the event that a business associate experiences a security breach, it must report the security breach to the covered entity with which it is working.[24]

States have their own security breach notification laws that may place additional security requirements on a covered entity.

State Laws and Preemption

States have their own laws regarding the privacy and security of health information. As a federal law, HIPAA preempts or supersedes these state laws when there is a conflict. However, HIPAA was meant to create a minimum standard of protection, so states are allowed to implement more stringent laws without being contrary to HIPAA.[25]

States often adopt more stringent protections for certain types of PHI. For example, in the context of legal proceedings, Florida only allows disclosure of substance abuse records pursuant to a court order. [26] In contrast, HIPAA allows disclosure pursuant to court order or a subpoena, discovery request or other lawful process not accompanied by a court order, as long as the requesting party provides certain assurances to the covered entity.[27] In this case, the more stringent state law

prevails over HIPAA's requirements.

In addition, when a conflict between HIPAA and a state law arises, DHHS can exempt the state law from preemption in certain circumstances.[28] Preemption is a complex topic; if preemption concerns arise, consult with your counsel.

The Network for Public Health Law

The Network for Public Health Law is a national initiative of the Robert Wood Johnson Foundation with direction and technical assistance by the Public Health Law Center at William Mitchell College of Law.

This document was developed by Kathleen Hoke, JD, Director of the Network for Public Health Law – Eastern Region and Mathew R. Swinburne, Staff Attorney, Network for Public Health Law – Eastern Region, University of Maryland Francis King Carey School of Law. *The Network for Public Health Law provides information and technical assistance on issues related to public health. The legal information and assistance provided in this document does not constitute legal advice or legal representation. For legal advice, please consult specific legal counsel.*

Endnotes

[1] 45 C.F.R § 160.103(2013).

[2] Id.

[3] Id.

[4] Id.

[5] 45 C.F.R. § 164.514(b)(2013).

[6] Id.

[7] Id.

[8] Id.

[9] 45 C.F.R. §164.502(a)(2013).

[10] 45 C.F.R §164.502(a)(1)(2013).

[11] 45 C.F.R. §164.512(b)(1)(i)(2013).

[12] 45 C.F.R. §§164.501(2013); 164.512(b)(1)(i)(2013).

[13] 45 C.F.R. §164.512(b)(1)(i)(2013).

[14] 45 C.F.R. §164.528(2013).

[15] 45 C.F.R. §164.502(b)(1)(2013).

[16] 45 C.F.R. § 164.306 (2013).

[17] 45 C.F.R. §§ 164.308;164.310;164.312 (2013)

[18] 45 C.F.R. § 164.308 (2013).

[19] 45 C.F.R. § 164.310 (2013).

[20] 45 C.F.R. § 164.312 (2013).

[21] 45 C.F.R. § 164.402 (2013).

[22] 45 C.F.R. § 164.404 (2013).

[23] 45 C.F.R. § § 164.406; 164.408 (2013).

[24] 45 C.F.R. § 164.410 (2013).

[25] 45 C.F.R. §160.203(2013).

[26] Fla. Stat. § 397.501(7)(a)(5) (2013).

[27] 45 C.F.R. §164.512 (e) (2013).

[28] 45 C.F.R. §160.203(2013).