HIPAA confusion and fear about protected health information

Joseph A. Woelfel
University of the Pacific, jwoelfel@pacific.edu

Follow this and additional works at: https://scholarlycommons.pacific.edu/phs-facarticles

Recommended Citation
HIPAA Confusion and Fear about Protected Health Information

Lead author: Joseph A. Woelfel, Ph.D., FASCP, R.Ph., Assistant Editor

For our Special Survival Guide on HIPAA, see our refresher course: "HIPAA Made Simple: A Survival Guide."

Background

The Health Insurance Portability and Accountability Act (HIPAA) became law in 1996. April 14, 2003 was the compliance date for all “covered entities.” These “covered entities” include health care providers, health plans, health care clearinghouses, and others having access to patient protected health information (PHI) in oral, written, electronic, or other format. PHI is any individually identifiable health information relating to a person’s past, present, or future health condition, provision of health care, and payment for that care. It includes any personal identifier such as name, Social Security number, address, medical record number, and telephone number.¹

HIPAA has created a national standard for patient privacy and confidentiality throughout the continuum of care. In the two years since its implementation, ongoing effort and expense have been realized to assure compliance. Yet, questions, confusion, and even fear still exist about HIPAA requirements and compliance.¹

Patients

Patients have the right to the protection of their personal health information. They also have the right to accurate, complete, thorough, and safe communication of that same personal health information between health professionals for their best care.

Patients must be given a “notice of privacy practice” statement by each HIPAA “covered entity” where the patient discloses protected health information. Patients must receive this notice on the first day any treatment or service is provided. Patients are not required to sign that they have received this notice but it is usual and customary for them to do so. If they choose not to sign or physically document their receipt, they must indicate they have received the notice and the service provider must document this acknowledgment in their records along with a reason for refusal to sign.¹

Each patient also has the right to access, inspect, and obtain a copy of their protected health information. Additionally, they are entitled to have the service provider amend their protected health information.¹

Pharmacists, Physicians, and Other Healthcare Professionals

Healthcare providers must be diligent in exercising and fulfilling HIPAA requirements. This is for their patients’ protection as well as their own personal and service providers’ protection. Failure to comply with HIPAA privacy law can result in civil or criminal penalties.¹

Each “covered entity” service provider must have an appointed Chief Privacy Officer responsible for developing and implementing policies and procedures, and assuring compliance with all HIPAA provisions. Service providers must also have a person responsible for both internal and external customer complaints, questions, and information.¹ Service provider employees must be trained on HIPAA requirements in their workplace and new employees trained when hired. All training must be documented.¹ Ongoing annual training on confidentiality issues is helpful for all employees. Real or hypothetical case-studies can serve as best practice models for education. An important reminder for all employees is that they do not have the right to access any PHI unless it is needed in the course of their serving patient care needs.

More...
Those professional caregivers who have a direct treatment relationship with the patient are legally and ethically authorized to receive, use, and transfer information using customary communication means. The law does not restrict this form of communication since it is in the best interest of the patient.  

At the same time, shared information must be the “minimum necessary” for communications between individuals involved with indirect care of a patient. Each situation in the continuum of care dictates that “minimum necessary” to assure both confidential and safety for the patient. Examples of situations where “minimum necessary” information should be provided include: waiting-room announcements such as a patient’s name only, restricted comments when in the presence of others who might overhear, discussions with an insurance carrier, providing a patient’s prescription to a family member or authorized friend on behalf of the patient. In these instances and all others, best judgment is required to protect patient confidentiality.

Each HIPAA “covered entity,” where the patient discloses their personal protected health information, must give a “notice of privacy practice” statement to the patient. HIPAA law requires that this notice be given in place of a formal consent form. Service providers who use consent forms cannot use these in place of the formal “notice of privacy.” Patients must be given this notice on the first day any treatment or service is provided. Patients are not required to sign that they have received this notice but it is usual and customary for them to do so. If they choose not to sign or physically document their receipt, they must indicate they have received the notice and the service provider must document this acknowledgment in their records along with a reason for refusal. The “notice of privacy” statement must be specific to the actual practices or services provided. At the time the patient receives this notice, the service provider should ask the patient about any additional confidentiality restrictions for use of their PHI. These must be documented in their records and respected. All documents must be retained for at least six years.

Providers might consider discussing the patient’s wishes about provider phone messages left on the patient’s message center or answering machine. HIPAA does not specifically prohibit providers from leaving messages. To safeguard patient privacy, the “minimum necessary” should be stated to limit the disclosed information. A provider might consider leaving only a message for the patient to call back.

Providing the personal health information of a minor to a parent or legal guardian is allowed by HIPAA, if such action is consistent with State or other applicable law, and the health care professional deems this to be in the best interest of the treated minor.

Disclosure of PHI is permitted by law in certain circumstances. These include: disclosures for certain public health activities for the purpose of preventing or controlling disease, for child abuse or neglect, for FDA-regulated product safety, quality, recalls, or adverse events, exposure to a communicable disease, health oversight activities to a health oversight agency, for judicial and administrative proceedings, certain law enforcement activities, and crimes.

Providers must furnish patients with a listing of any instances when their personal information was disclosed outside of their treatment related routine disclosure. This is a patient right. These non-routine disclosures must always be documented in their records. Service providers must give the patient this listing within 60 days of their request and include requesting name, date, address, description, and reason for the disclosure. Providers must obtain documented patient authorization before they can disclose any PHI not authorized under HIPAA provisions. The authorization should contain a description of the information disclosed, reason for disclosure, individual or agency receiving the information, and an expiration date for use of the information. If the purpose of the disclosure is for marketing, remuneration must be included in the documentation. Authorized documentation must be made prior to any disclosure.

Patients requesting access to their personal protected health information may be required by the service provider to request this access in writing. Patients are allowed access, inspection, and copies of their records. Service providers are allowed up to 30 days to act on the patient’s request. Cost-based fees can be charged to the patient for supplies, labor, and postage associated with copies.

Patients requesting that their personal protected health information be amended by the

More...
service provider may do so. The provider may ask that the request be in writing and the reason for amendment stated. Providers have up to 60 days to respond. Providers may refuse to amend the information for a variety of reasons including that the information is accurate and complete.¹

**Commentary**

The application of and compliance with HIPAA requirements protects both patients and health care professionals in assuring confidentiality. The HIPAA Privacy Rule has created the legal expression for our professional codes of ethics. Using these ethical guidelines for serving patients can alleviate both confusion and fear about HIPAA.

---

**References**


---

Users of this document are cautioned to use their own professional judgment and consult any other necessary or appropriate sources prior to making clinical judgments based on the content of this document. Our editors have researched the information with input from experts, government agencies, and national organizations. Information and Internet links in this article were current as of the date of publication.

Cite this Detail-Document as follows: HIPAA confusion and fear about protected health information. Pharmacist’s Letter/Prescriber’s Letter 2005;21(9):210914.