Access, Use, and Disclosure: HITECH's Impact on the HIPAA Touchstones

Save to myBoK

By William M. Miaoulis, CISA, CISM

The Health Information Technology for Economic and Clinical Health (HITECH) Act significantly changes how organizations will address the access, use, and disclosure of protected health information (PHI). It also establishes a national breach notification requirement when information is accessed in an unauthorized or inappropriate manner.

Access

The HIPAA privacy rule gave patients the right to access and receive a copy of their personal protected health information from a covered entity. The original HIPAA regulations provided the following right or access:

> An individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set.

HITECH extends the requirements for covered entities that manage protected health information via electronic health records (EHRs). Organizations must provide the patient (or individuals or entities authorized by the patient, such as doctors and personal health record services) with an electronic copy of their file.

Organizations must now ask themselves the following questions when it comes to this requirement:

- What is the EHR? Data exist electronically in numerous locations. Organizations should determine what constitutes the EHR and understand which systems will be accessed to provide the information, such as the radiology system, the laboratory system, or the primary clinical system.
- Does the EHR have the capability to comply with requests for electronic access?
- How will patients receive an electronic copy of the data? Will they use a Web portal, a CD, an e-mail, a thumb drive?
- What will the format be for electronic access? Will the organization provide information in native format, or will it use PDF or proprietary data formats?
- What security protections will be employed to secure the electronic access (e.g., encryption, passwords, hash totals)?
- Will the data be marked to document they were issued to the patient and have not been modified?
- Will the data be time stamped?
- Will the organization instruct patients on protecting this electronic information?

The regulations do not specify what form of electronic access covered entities must provide. Further, they do not specify that organizations have a responsibility to assist or train patients on the security risks associated with the electronic records entrusted to them. Organizations must make these determinations themselves, including how to minimize risks to that data to the degree possible.

Although HITECH mandates the ability to receive information electronically, it is important to note that the regulations do not change the circumstances in which access to the information may be withheld. For example, organizations can still deny access to psychotherapy notes.

A patient request also can be denied if an organization determines that the information requested is reasonably likely to endanger the life or physical safety of the individual or another person.

The timeline for providing information in electronic form is dependent on when the organization first implements an EHR. Organizations currently using EHRs were responsible for providing information electronically starting February 18, 2010.

Use

HIPAA and HITECH place restrictions on how organizations use PHI. The HIPAA definition will assist in defining its appropriate use:

> *Use* means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

The HITECH regulations impose additional controls or requirements on the use of the information, specifically expanding the concept of minimum necessary information. HITECH requires healthcare organizations limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or to the minimum necessary.

The HIPAA privacy regulations have always required organizations provide only the minimum necessary information to accomplish a specific task. HITECH clarifies that the covered entity disclosing the PHI is required to make the minimum necessary determination.

Although the Department of Health and Human Services secretary must issue guidance on the minimum necessary concept within 18 months of enactment (August 2010), the requirements as specified by HITECH are in effect now, and organizations should begin their compliance efforts with a review of their current access processes and limit information to the minimum necessary.

Once current processes have been reviewed, organizations should:

- Document the location of their information (e.g., home computers, cell phones, files sent externally, application systems, databases, and spreadsheets)
- Ensure that users accessing application systems have the minimum necessary to accomplish their job
- Document and review the access levels given to various workforce members (HIPAA security requirement)
- Review who has access to raw database data and document the reports created (i.e., crystal reporting)
- When appropriate remove identifiers from PHI when responding to requests for uses (internal) and disclosures (external) and limit access to the field level (e.g., do they need diagnosis, lab values, Social Security numbers, birth dates versus birth month and year, patient name, etc.?)
- Review all files sent externally, document what is contained on the file, and apply minimum necessary standards to limit information

Traditionally many organizations have given access to information that is not needed, and all too often organizations have had difficulty documenting the access granted to internal users and other organizations. The new federal breach notification requirements offer one more reason to review and adjust policies and procedures as necessary; the upcoming Red Flags Rule, which requires most healthcare organizations establish medical identity theft prevention measures, is another.

Disclosure

When organizations send or share information outside the organization, they are disclosing information. HIPAA defines disclosure as:

> the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

While HITECH does not change this definition, it does change the accounting of such disclosures for organizations using an electronic health record.

Prior to HITECH, organizations were required to account for nonroutine disclosures. Now organizations that use EHRs must account for all disclosures, including those for treatment, payment, and healthcare operations.

Organizations also must account for disclosures made by their business associates or provide individuals with a list of their business associates and their contact information. HITECH shortens the accounting period to three years.

It is unclear if HITECH requires organizations to account for internal use. Although this is part of treatment, payment, or healthcare operation, the legislation does not specifically address authorized, appropriate internal use. It only addresses external disclosure.

Based on the definitions, it would appear that only accounting of disclosures would apply. HITECH calls for the Office for Civil Rights to issue the actual regulations modifying the HIPAA privacy rule's accounting of disclosures provisions.

Providers who implement EHRs after January 1, 2009, must comply by January 1, 2011. Those who use EHRs purchased prior to January 1, 2009, have until January 1, 2014, to comply.

This staggered scheduled is based on the assumption that earlier EHR systems may not have the necessary functionality. The extended deadline gives vendors extra time to retrofit features to support HITECH measures.

Breaches

Organizations must also consider inappropriate access by their workforce members when reviewing their internal access policies and procedures. It is important to note that from the original HIPAA compliance date to the present, the compliance issue investigated most often by the Office for Civil Rights is the impermissible use and disclosure of PHI.

If an internal use is unauthorized or constitutes a breach, then the HITECH breach notification provisions require that the organization notify the breach victims and the Department of Health and Human Services. The interim final rule on breach notification, published by Health and Human Services, defines a breach as:

> the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA privacy rule, and where the security or privacy of the PHI is compromised.

The regulation includes a harm threshold. No compromise of security or privacy occurs if there is no risk of "significant financial, reputational or other harm to the individual." In such cases the organization is not required to notify the individual, but it is required to document its risk analysis.

The definition of breach excludes unintentional access, inadvertent disclosure, and disclosure where the recipient would be unable to retain the PHI.

For example, if an authorized user looking up the record of John A. James instead calls up the record for John B. James, this is not a breach. However, if an authorized user breached John B. Smith's information willfully and without a business need, this could be a reportable breach of information.

Assessing such incidents should lead organizations to create a standardized process for evaluating breaches and their risk.

William M. Miaoulis (wmiaoulis@phoenixhealth.com) is a subject matter specialist at Phoenix Health Systems.

Article citation:
Miaoulis, William M. "Access, Use, and Disclosure: HITECH's Impact on the HIPAA Touchstones" *Journal of AHIMA* 81, no.3 (March 2010): 38-39; 64.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.