HIPAA and the EHR: Making Technical Safeguard Changes

Save to myBoK

by Joseph Fodor

As electronic health records (EHRs) become more commonplace in healthcare, changes, adjustments, and improvements will be inevitable. When designing, implementing, upgrading, or remediating an EHR system, your organization's implementation team should consider the impact of complying with the HIPAA security rule by April 2005.

The HIPAA security standards apply to electronic protected health information (PHI) as it relates to health plans, healthcare clearinghouses, and healthcare providers that transmit any health information in electronic form in connection with a HIPAA-covered transaction. This article will explore what your organization should consider when making system changes to be in compliance with HIPAA security technical safeguards.

Understanding Standards and Safeguards

HIPAA security standards address the confidentiality, integrity, and availability of electronic PHI in three main categories—administrative, physical, and technical. This discussion is limited to the technical safeguards as they relate to the EHR. Defined in the technical safeguards are standards that in most cases have associated implementation specifications, some of which are required and others that are addressable. Addressable implementation specifications are to be implemented if they are deemed reasonable and appropriate. Those standards that do not have an associated implementation specification are by default required.

Technical safeguards include:

- Access to electronic PHI (accessing information through unique user identifications and controlling system access)
- Monitoring or auditing access
- Helping to ensure data integrity and detecting any alteration or destruction of electronic PHI
- Authentication (identity confirmation for individuals and entities)
- Monitoring the transmission of electronic PHI over an open network

Of the technical safeguards, audit controls and authentication are two standards that do not have associated implementation specifications, but they must be implemented.

Determining Policies and Procedures

Access control policies and procedures must exist over the EHR. There must be a policy that addresses the minimum amount of information necessary for an individual to perform his or her job, and a procedure must be in place to grant that access. For instance, a manager should authorize and approve role-based access to the EHR according to appropriately approved and documented policies.

A provision needs to be made for identifying and tracking activity by user via a unique user name or number. This is addressed by login name into the EHR, which is generally six to ten alpha-numeric characters, a combination of the user's first and last name, or a less meaningful combination of characters and numbers. The benefit of using the user's name when performing a review of the audit logs is that it makes it easier to quickly identify which user accessed which data. The risk to using a name is that it may be easier to guess that user's password and thereby circumvent security.

Procedures must exist to verify that a person or entity seeking access to electronic PHI is who he or she claims to be. This verification typically takes the form of a unique user ID and password. EHR systems must provide for audit logging controls that record and examine activity of the use of electronic PHI. Additionally, there must be procedures for obtaining necessary electronic PHI during an emergency. With regard to EHR systems the significance is clear. If the system is not available,

patient care could suffer. In light of events like power outages or terrorist attacks, it is imperative that contingencies exist for these types of events as well as hard drive and network failures.

Several addressable implementation specifications such as automatic logoff, encryption, and decryption are highly dependent on the EHR systems that have been deployed and the location of the workstations that access the EHR. For instance, a security executive may determine that a terminal located in an emergency room may be set to automatically log off after a greater period of time or not at all, as opposed to a workstation in a less critical patient care area that is set to lock out a user after a shorter period of inactivity.

Evaluating Specifications

There are two encryption and decryption specifications. One is relevant for electronic PHI at rest or data stored on a device. Examples may include workstations, tablet PCs, personal PCs, personal digital assistants (PDAs), or other enablers of EHR technologies.

The other encryption specification addresses data as it is being transmitted. Encryption methods are usually deployed for data that is transmitted wirelessly or remotely, but encryption is not likely if the data is transmitted across a local area network (LAN) or stored on a device. Management must evaluate whether LAN traffic should be encrypted, whether policies should exist restricting the storage of electronic PHI on various devices, and whether encryption technologies should be implemented for portable terminals, laptops, or PDAs.

Another set of addressable implementation specifications includes integrity controls over stored and transmitted electronic PHI. With respect to stored data, mechanisms should be in place to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner. For transmitted data, measures should ensure that this data is not improperly modified without detection. The EHR system may be capable of tracking all changes made to the electronic PHI. Addressing the transmission encryption specification will go a long way toward mitigating the risk that electronically transmitted PHI is improperly modified.

Technical safeguards defined within the final HIPAA security rule must be addressed as they relate to EHR systems. The covered entity must ensure the confidentiality, integrity, and availability of the EHR. In addition, covered entities should protect this information against any reasonably anticipated threats or hazards to the security or integrity of the data, protect it against any reasonably anticipated uses or disclosures that are not permitted, and ensure that its work force is in compliance with the regulations. With appropriate planning and execution an entity can comply with the HIPAA security regulations and help contribute to effective patient care.

Joseph Fodor *(Joseph.Fodor@ey.com) is a senior manager with Ernst & Young.*

Article citation:
Fodor, Joseph. "HIPAA and the EHR: Making Technical Safeguard Changes." *Journal of AHIMA* 75, no.1 (January 2004): 54-55.
