Transition to electronic health records, means updates to security standards

By: Heather L. Stewart, RHIT, CCS, CHPS
Health Informatics and Coding Consultant
RB Health Partners, Inc.

For providers, patient confidentiality and record security are important components of daily operation. However, many providers may not follow the most current security requirements. The Health Insurance Portability and Accountability Act (HIPAA) standards have been updated to ensure that covered entities (CEs) protect the confidentiality, integrity, and availability of all electronic personal health information (ePHI). This includes protections against anticipated threats or hazards to the security or integrity of ePHI. These updates provide CEs guidance regarding implementation of customized security measures based on the size and complexity of a covered entities technical infrastructure and software security capabilities. This customization is determined by the CEs based on the probability and criticality of the risk potentials determined after analysis.

The Office of Civil Rights (OCR) began Phase 2 audits in July 2016 for CEs and in the Fall of 2016 for business associates (BAs). Audits focused on either Security Rule controls or Privacy and Breach Notification rule compliance. The goal of these audits is to enhance industry awareness of requirements, identify problem areas, develop tools and guidance to assist CEs with compliance evaluation and breach prevention. A breach is the access, use, or disclosure of unsecured protected health information (PHI), by means not permitted by the HIPPA, which poses a risk of financial or other harm to the affected person. Audit processes and results will also be utilized to develop a permanent audit program. Thus, the importance of understanding and implementing the newest standards is of the utmost importance for all CEs and their BAs.

There are three areas of safeguards that must be reviewed, these are: Administrative, Physical, and Technical. Each area has standards with required and/or addressable implementation specifications. CEs must implement all required specifications and assess the appropriateness of all addressable specifications in relationship to its contribution to protecting the electronic protected health information (ePHI). If implementation of an addressable specification is not reasonable or appropriate the CE must document why and implement an equivalent alternative measurement when possible.

The administrative safeguards cover the security management process. This includes the implementation of policies and procedures to prevent, detect, contain, and correct security violations. These policies include workforce security, sanctions, information access management, security and awareness training, disaster recovery and emergency operation planning and incident response and reporting. Implementation specifications also include the completion of a risk analysis. The risk analysis is a detailed and accurate assessment of the potential vulnerabilities to the confidentiality, integrity and availability of ePHI. Another required specification is the appointment of a facility Security Officer. The Security Officer, in conjunction with the Privacy Officer, is responsible for the development and implementation of a facility's privacy and security policies and procedures. Lastly, the administrative safeguards update the requirements of the CE and their BAs. Business associate agreements (BAAs) should be reviewed to ensure that components of the safeguards are addressed and assurance is made that the BA will abide by the requirements.

The next safeguards are related to the physical environment and devices in which the ePHI is maintained and stored. Collectively, these are known as the physical safeguards. CEs should have policies and procedures in place to limit access to the electronic information system and areas where records are stored. This is done by implementation of facility security plans, access controls and contingency operations. Important components of physical safeguards are workstation use and security. Workstation use policies will address the way workstations are used and what applications and programs are acceptable to run while workstation security policies address restrictions to the workstation access. CEs must also address controls for computers and other devices or media where ePHI may be stored. Policies regarding specifications on proper disposal or re-use of any devices which stored ePHI. The final addressable physical specification is related to access control and validation. CEs must review and implement policies and procedures regarding limiting access to ePHI based on a person's role or function, as well as access to their systems and programs for testing and revisions.

The last set of safeguards are those related to the technical applications utilized to secure ePHI and the systems in which it is maintained. The first required standard is the implementation of access and audit controls. CEs are required to ensure that only authorized people are allowed access. This is accomplished by providing each person a unique user identification. The unique user identification allows for identifying and tracking each user. Audit controls are hardware, software or other processes that can record and review activity in the systems containing ePHI. Next, CEs must implement policies to protect the integrity of the ePHI. Policies should address mechanisms in place to ensure that ePHI has not been improperly altered or destroyed. Just as CEs have specific standards regarding how to properly correct entry errors in paper documentations, the same must be done for electronic documentation. Lastly, technical security measures must address the potential unauthorized access of ePHI transmitted via electronic communication networks. This is most often completed through a process called encryption. CEs should implement policies related to when encryption is required and the process for ensuring encryption of ePHI prior to transmission. It is best practice that CEs utilized a HIPAA compliant secure email service with encryption capabilities as specified in the regulatory standards to transmit any form of ePHI.

In conclusion, CEs must take an active role in identifying areas of potential risks and vulnerabilities to the confidentiality and integrity of ePHI. Then implement security measures reduce the likelihood of these potential risks and vulnerabilities will lead to a breach of ePHI. Compliance with HIPAA standards protect the CE and their patients from potential threats to ePHI and ensures that patient confidentiality and record security continue to be important components of daily operation.

For more information about this or related topics or health information management consultant services please contact the author at heather@rbhealthpartners.com or Robin A. Bleier, President of RB Health Partners, Inc. at robin@rbhealthpartners.com 727.786.3032.