Compliance Update - 03/31/16

Phase 2 HIPAA Audits

It's time to review and complete your policies and procedures before the U.S. Department of Health and Human Services (HHS) begins Phase 2 HIPAA audits later this year. The Health Information Technology for Economic and Clinical Health (HITECH) Act requires HHS to perform audits of covered entities and Business Associates (BAs) to make sure they are complying with the Health Insurance Portability and Accountability Act (HIPAA); which includes Privacy, Breach Notification, and Security Rules. The HHS Office of Civil Rights (OCR) began audits in 2012 and shares the results of 115 covered entity audits from this pilot program. By reviewing the initial audit findings, employers can identify the focus of previous HIPAA audits and prepare accordingly.

With respect to the Security Rules, the OCR initial audit found most entities failed to perform a comprehensive and accurate security risk assessment. Without an assessment, it is difficult to maintain the documentation of an internal risk analysis or the associated management plan to detail how the organization intends to manage the risks. Other concerns included a lack of media management and audit controls, including controls for the disposal of protected health information (PHI).

As to the Privacy Rule, most covered entities failed to meet the audit protocol related to providing a Notice of Privacy Practices and having executed Business Associate Agreements (BAAs). Also lacking were procedures for the use of PHI as it relates to internal access, applying the "minimum necessary" rule, documented workforce education and training on an annual basis, or the application of sanctions after a failure to safeguard PHI.

Phase 2

The OCR's Deputy Director of Health Information Privacy, Deven McGraw, reported recently that Phase 2 audits have begun. The OCR is at the early stages of this Phase and is currently confirming addresses for those Covered Entities (CEs) and BAs that will receive questionnaires. The OCR will then select a diverse pool of audit candidates from information gathered on this questionnaire. The Phase 2 audits will include at least 200 desk audits, the focus of which will be on specific provisions of the rules, and conduct 10 to 25 full-scale onsite audits.

Expect updates to the current audit protocol used in 2012. Updates will occur as a result of the HIPAA Omnibus Rule and provide more guidance in evolving areas such as cyber-security. We should see the proposed changes in April 2016, with a comment period allowed, with final changes implemented yet in 2016 before Phase 2 audits begin. It is prudent to familiarize your team with the current audit protocol.

Next Steps

First, be on the lookout for the OCR's email being sent to request contact information. OCR will follow up with the pre-audit questionnaire sent to select covered entities for desk audits and on-site audits. It is important for privacy officials and executives to take immediate action. Keep in mind, the email may be incorrectly classified as spam. OCR expects entities to check their junk or spam email folder for emails from OCR. If an entity does not respond to OCR's request to verify its contact information or pre-audit questionnaire, OCR will use publicly available information about the entity to create its audit subject pool. Therefore an entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.

This HIPAA Audit Checklist can serve to get you started.

- Written and adopted Policy and Procedures for privacy, security and breach notification.
- Notice of Privacy Practices: Review the Notice of Privacy Practices- does it meet content, posting and distribution requirements?
- Workforce Training and Education. Review training materials and update as appropriate. Document evidence of workforce training and education is occurring.
- Protect Physical PHI. Review use of paper shredders, copiers, storing PHI, as well as access and security of physical PHI.
- Review the uses and disclosures of PHI to ensure the minimum necessary amount of PHI is used and the disclosure is appropriate internally and externally to the business.
- Security Risk Assessment - Analysis and Plan. Compile documentation that demonstrates a risk assessment plus, analysis has been conducted and that plans were developed and implemented based on the assessment and analysis. The plan would include timelines for implementing security controls and the identification of risks and vulnerabilities. It would be ongoing as business changes dictate.
- Transmission Security. Review how electronic protected health information (ePHI) is protected and the devices used to transmit including if encryption is used.
- Review policies and procedures for the use, reuse, disposal, storage and back up of devices, and systems that contain ePHI.
- Facility Security. Maintain an inventory of where PHI is located and updates to a facility security plan that occurs as new business or IT equipment is acquired.
- Breach Notification. Ensure breach notification policy complies with the requirements of the standard and maintain documentation of notifications. Documentation of incident review, responses, mitigation, investigation, and the application of a risk assessment to determine if a breach requires notification are all required.
- Compile a list of all BAs and confirm an associated BAA is executed and conforms to current practices with the BA.

Penalties

In addition to reputational repercussions for the business, HIPAA and HITECH have significant economic penalties. For instance, HHS can impose civil penalties of $100 to $50,000 per violation with the total amount, imposed on an entity for all violations of an identical requirement, not to exceed $1.5 million during a calendar year. Keep in mind the maximum fine is for each separate violation of each provision and most compliance failures involve numerous provisions.

Criminal Penalties are enforced by the Department of Justice (DOJ). These apply when a person knowingly discloses health information in violation of the provisions. The penalties include a fine of not more than $50,000, imprisonment of not more than one year or both, and can extend to a fine of $250,000 and imprisonment of up to ten years, or both, when there is intent to sell or use health information for personal gain or malicious harm.

Effective February 18, 2009, the HITECH Act authorized all state attorneys general to bring civil actions in federal court for violations of HIPAA to protect the interest of residents in their states.

Any audit can be disruptive to business as usual. It's prudent to prepare now. Become familiar with the audit protocol, document requirements, and correct procedures. Make the necessary changes internally to be prepared to respond quickly.

Thank you,
WageWorks

WageWorks
1100 Park Place 4th Floor
San Mateo, CA 94403
servicenotice@wageworks.com

15017 (3/2016)