HIPAA Privacy and Security Audits Underway

Authors

Leslie J. Anderson
Jessica Forbes Olson

Related Services

Benefits and Compensation

July 23, 2012
Attorney Articles

The Health Information Technology for Economic and Clinical Health Act (HITECH) requires the Secretary of the U.S. Department of Health & Human Services (HHS) to provide for periodic audits to ensure that covered entities (such as group health plans) and their business associates comply with the HIPAA privacy and security requirements. Those audits are underway.

HHS recently published an audit protocol for use by Office of Civil Rights investigators to determine compliance by covered entities or business associates with (1) the Privacy Rule; (2) the Security Rule; and (3) the Breach Notification Rule. The audit protocol is available here.

Below we describe some of the highlights of the audit protocol.

I. Privacy Rule

The audit protocol describes how investigators reviewing Privacy Rule compliance will, among many other things:

- Review the group health plan's HIPAA plan amendment to ensure it properly restricts uses and disclosures of PHI by the plan sponsor.
- Analyze the privacy notice to ensure it contains all the required elements under the Privacy Rule.
- Review privacy policies and procedures.
- Review HIPAA privacy training documentation, including documentation showing that training was completed.
- Evaluate compliance with individual rights to access, amend and receive an accounting of disclosures of their PHI.
- Observe whether administrative, technical and physical safeguards are in place to protect PHI.
- Determine whether PHI access is restricted properly under the minimum necessary rule by reviewing job descriptions of workforce members with access to PHI and ensuring that they have access to only the PHI necessary to perform their job.
- Determine whether PHI disclosed, for example, to business associates, is limited under the minimum necessary rule to the amount reasonably necessary to achieve the purpose of the disclosure.

II. Security Rule

The key theme of the HIPAA security audit protocols is that HIPAA security compliance is not a one-time event – it is an ongoing process, based on changes to the security environment. The HIPAA security protocols stress this point by noting over 40 times that different HIPAA security requirements, including the risk assessment, must be conducted on a “periodic basis.” The security protocols describe how investigators reviewing Security Rule compliance will, among many other things:

- Evaluate the risk assessment and determine if it has been conducted on a periodic basis.
- Inquire as to whether procedures exist to review information system activities, such as audit logs, access reports and security incident tracking reports and determine whether those procedures have been updated on a periodic basis.
- Inquire as to whether a HIPAA security official has been designated and review the documentation of the security official’s responsibilities.
- Review whether HIPAA security policies and procedures are updated periodically.
- Determine whether HIPAA security training is conducted whenever there are changes in technology and practices.
- Review whether security incidents have been properly identified and documented.
- Inquire as to whether a process is in place to ensure business associate agreements include the required HIPAA security language.
- Observe workstations that access electronic PHI and ensure they are located in secure areas and protected with physical security controls such as cable locks and privacy screens.
- Review the method of tracking the location and movement of media and hardware containing ePHI.
- For implementation specifications that are “addressable” rather than “required,” determine if there is documentation of where the specification was not fully implemented and the rationale behind that decision.

III. Breach Notification Rule

The audit protocol describes how investigators reviewing Breach Notification Rule compliance will, among many other things:

- Determine whether a process is in place to notify individuals, the media and the Secretary of HHS when required under HITECH.
- Review whether HITECH breach notification procedures are included in business associate agreements.
- Review documentation of uses and disclosures that were determined to not be breaches under HITECH and the documentation supporting such determinations.

IV. Conclusion

We have described only some of the highlights of the new audit protocol. Group health plans and their business associates will want to use the audit protocol to

conduct a self-audit to determine whether their HIPAA privacy, security and breach notification documentation and procedures are in compliance with applicable requirements. Because of health care reform compliance, employers may have been less focused on HIPAA Privacy, Security and HITECH compliance. The audit protocol is a reminder that there are many complex and ongoing privacy and security compliance obligations for group health plans.