Are You Ready for a HIPAA Audit?

Save to myBoK

By Lou Ann Wiedemann, MS, RHIA, CHDA, CDIP, CPEHR, FAHIMA

Editor's Note: The following is an excerpt from the new "External HIPAA Audit Readiness Toolkit" developed by AHIMA. The full toolkit is free for AHIMA members.

THE HITECH OMNIBUS Rule mandated that the US Department of Health and Human Services (HHS) conduct periodic audits on privacy and security compliance. The HHS Office for Civil Rights (OCR) added HIPAA-covered entities (CEs) and their business associates (BAs) to the audit schedule in March 2016 as a part of Phase 2 implementation.

These ongoing audits are an important compliance measuring tool for OCR. Combined with other enforcement tools, such as investigating complaints filed with OCR, performing education and outreach, and working with the Department of Justice (DOJ) to investigate criminal complaints, OCR is in the midst of its toughest crackdown yet on non-compliance with HIPAA.

Throughout 2017, OCR plans to use the audit program to assess the HIPAA compliance efforts of a range of HIPAA CEs and their BAs. The audits present an opportunity to examine mechanisms for compliance, identify best practices, and discover risks and vulnerabilities to patients' protected health information (PHI). The audits will also assist in enhancing overall industry awareness of compliance obligations. Through the use of OCR's audit protocol for self-evaluations, CEs and BAs can monitor their compliance with the standards and specifications of the HIPAA rules.

This change of the regulation to include business associates also increases the potential for an audit by expanding regulators' efforts. Compliance with HIPAA will no longer be initiated only by complaints and self-reported breaches. OCR will use desk and on-site audits as a part of their enforcement arsenal. While these audits are not intended to be investigations, they have the potential to reveal a serious compliance issue that could lead to a separate enforcement investigation and potential action by OCR.

Preparing for On-site Audits

On-site audits began in January 2017, evaluating CEs and BAs against a comprehensive set of HIPAA compliance controls. CEs can be chosen for a desk audit, an on-site audit, or both. Receiving an OCR desk audit does not mean that the CE will not also be selected for an on-site audit. Nor does being selected for a desk audit remove the CE from the selection pool for the on-site audits.

In order to prepare for a potential audit, the CE or BA should take proactive steps that demonstrate ongoing compliance with the HIPAA Privacy and Security Rules. CEs and BAs should ensure that all processes are well documented. Lack of adequate documentation may lead to substandard audit results. AHIMA's new "External HIPAA Audit Readiness Toolkit" advises CEs and BAs to organize the elements of their HIPAA compliance efforts in a centralized manner. This means supporting documentation is easily accessible to respond to any external audit of privacy and security practices.

The toolkit advises CEs and BAs to consider creating a formal HIPAA compliance plan to centralize the supporting documentation for HIPAA audit readiness, and also to review the plan annually to detect gaps or add revisions. Completion of the plan will help the CE and BA respond to protocol criteria as well.

The CE or BA will want to ensure that the following elements are identified, documented, and maintained in its HIPAA compliance efforts:

- Up-to-date privacy officer job description
- Implementation of a HIPAA oversight committee
- Documentation of key policies and procedures

- Documentation of HIPAA training, education, and awareness activities
- Identification of key metrics for reporting compliance activities
- Well-articulated access audit plan
- Identification of leadership reporting tools

The Future of HIPAA Audits

As the healthcare industry constantly changes, so too do regulatory and legal actions. A strong auditing and monitoring program can help mitigate legal interventions and avoid potential sanctions. For example, new areas of possible focus for CEs and BAs are user access audits. These types of audits are beginning to appear across the industry as disgruntled or terminated employees improperly access the PHI of management/executive/board members, noteworthy/high-profile accounts, random patient accounts, or employee patients.

Ensuring privacy and security is not an exact science and there will be challenges ahead. One challenging area many are already facing is the need to continually update programs. There are many areas in which CEs and BAs can choose to focus their preparation efforts. Some may choose user access audits as a focus, whereas others may have identified theft of devices as a more pressing threat. But CEs and BAs need to consider which activities will be the most beneficial to achieve the highest level of compliance.

In addition, just keeping abreast of all the federal and state regulations and protocols may require serious staff time and rigor. Potential auditees need to ask themselves early on if they have set aside enough time and staff to work on compliance and achieving optimal outcomes.

Download

Read the Complete HIPAA Audit Readiness Toolkit

AHIMA's External HIPAA Audit Readiness Toolkit was created and designed to be a single resource for details on preparing for and passing an audit of privacy and security practices. Since the Office for Civil Rights (OCR) announced its Phase 2 HIPAA Audit Program, selected entities can expect to be audited on their compliance with either the privacy or security rules. This toolkit, free for AHIMA members, enables the reader to understand the requirements for HIPAA Phase 2 audits and offers guidance regarding audit preparation and recommended practices.

Lou Ann Wiedemann (lou-ann.wiedemann@ahima.org) is vice president of HIM practice excellence at AHIMA.

Article citation:
Wiedemann, Lou Ann. "Are You Ready for a HIPAA Audit?" *Journal of AHIMA* 88, no.4 (April 2017): 26-27.