What is Security Auditing?

Save to myBoK

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

The HIPAA security rule includes a requirement for audit controls and to monitor and manage ongoing security for a variety of processes. But the requirement for internal audit was changed to "information security activity review," and there is no other specific reference to auditing. So what are the "security audits" people are talking about and what are the "security auditing" services people are trying to sell?

Auditing in General

Before looking at the specific HIPAA requirements that might refer to auditing, it is helpful to understand the general meaning of audit. With respect to security, audit generally means an in-house review of the records of system activity (e.g., log-ins, file accesses, and security incidents) maintained by an entity to reduce wrongful disclosure, damage, or destruction of data. In the financial arena, an audit is performed to examine an entity's financial books and records (general ledger, check registers, invoices, receipts) to protect against errors and fraud. The term "internal audit" is frequently used to convey the notion of a formal investigation into an activity.

Possible HIPAA Meaning for Auditing

With respect to HIPAA, there are several possible meanings for what some may call auditing. Those responsible for information security should understand the actual requirements and how an audit fits into compliance. Auditing may be used to describe:

- **Security risk analysis** (§164.308(a)(1)(ii)(A))—"an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by a covered entity." It identifies gaps, or vulnerabilities, and threats that might exploit those vulnerabilities. HIPAA specifically mentions in the preamble that threat assessment is a component of risk analysis.[1] The purpose of a risk analysis is to factor into selection of controls the probability that a threat exploiting a vulnerability will result in a critical impact to the entity. Merely performing a security audit will probably not include the threat assessment component and could result in the selection of controls that are not necessarily designed to be reasonable and appropriate for the entity's specific needs.
- **Information system activity review** (ISAR) (§164.308(a) (1)(ii)(D))—"regular review of information systems activity, such as audit logs, access reports, and security incident tracking reports." The preamble advises that this language was adopted in place of internal audit, which had rigid formal connotations.[2] Despite the change from internal audit to ISAR, this process is probably closest to what security auditing is, except that it generally is not what people are selling as auditing services. ISAR is generally an ongoing monitoring process, whereas audit suggests a focused review of monitoring at a point in time. ISAR is key to risk management, which is the implementation of security measures sufficient to reduce risk to reasonable and appropriate levels.
- **Evaluation** (§164.308(a)(8))—"a periodic technical and nontechnical evaluation, based initially on the HIPAA standards, and subsequently in response to environmental or operational changes affecting security." Evaluation may actually be the closest HIPAA standard to what is typically meant by audit. The initial evaluation focuses on vulnerabilities. Subsequent periodic evaluations are often performed after an event or incident has triggered the need to consider possible enhancements to security.
- **Audit controls** (§164.312(b))—"hardware, software, and/or procedural mechanisms that record and examine activity in information systems." Audit controls produce audit logs or trails that are reviewed and analyzed to determine if there have been inappropriate accesses, intrusions, and other efforts to thwart security measures. The audit logs are documentary evidence of system access. While audit control procedures may be called auditing, they are performed as an inherent part of the system and should be reviewed regularly by the information security official for potential problems warranting further investigation.

Why Does It Matter?

As with any other internal activities to which resources are applied or with services one is looking to purchase, the information security official should be aware of what is required and what a vendor is selling. This is not to suggest that auditing isn't necessary or that auditing services are invalid or inappropriate—rather, it ensures that auditing and auditing services meet your organization's needs.

Help from NIST

The National Institute of Standards and Technology (NIST), which is a part of the US Department of Commerce and tasked to provide standards for federal government technology, has recently released "An Introductory Resource Guide for Implementing the HIPAA Security Rule." The resource guide summarizes key activities in evaluating, selecting, and implementing security measures for HIPAA. It provides references to other NIST documents for more detailed, technical analysis of controls. It also provides sample questions to help conduct the risk analysis. Readers should be forewarned, however, that the resource guide is primarily focused on implementing HIPAA in the federal government, and although it does help you ask the right questions, it does not provide the answers. For example, under audit controls (§164.312(b)), it suggests you ask yourself:

- What should be audited?
- How long should audit trails be maintained?
- How will exception reports be reviewed?[3]

The NIST resource guide provides good questions to ask, but it does not tell you what security measures are right for your environment.

Interestingly, the NIST document uses the term "auditing" only in the context of audit controls (§164.312(b)) and only addresses ISAR (§164.308(d)) under that section. This resource guide is available for downloading at http://csrc.nist.gov/publications/nistpubs.

Buyer Beware

If you are still feeling confused by what auditing means, perhaps you are not alone. The best advice is to adhere closely to the definitions provided in the HIPAA standards, and if you buy auditing services, investigate the products and understand what you are buying.

Notes

1. Department of Health and Human Services. "Health Insurance Reform: Security Standards; Final Rule." *Federal Register* 68, no. 34. (2003): 8347.
2. Ibid.
3. National Institute of Standards and Technology. "An Introductory Resource Guide for Implementing the HIPAA Security Rule (Draft)," NIST SP 800-66. Available online at http://csrc.nist.gov/publications/drafts/DRAFT-sp800-66.pdf.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "What Is Security Auditing?" (HIPAA on the Job column) *Journal of AHIMA* 75, no.10 (Nov-Dec 2004): 58-59.

Driving the Power of Knowledge