Keeping It Private: Staying Compliant with the HIPAA Privacy and Security Rules

by Jonathan P. Tomes, JD

HHS's renewed interest in auditing for compliance is a good reminder to covered entities to ensure their privacy and security programs are up to date.

The Department of Health and Human Services' (HHS) announcement of a new program to audit compliance with the HIPAA privacy and security rules has, quite properly, generated a great deal of concern for covered entities, especially because the Office for Civil Rights (OCR) has noted that major violations detected by the audits may lead to civil monetary penalties.

Of course, not every covered entity (or business associate, now that HITECH subjects them to HIPAA audits) will be audited at any time in the near future. The HHS contract with KPMG, one of the big four accounting firms, envisions as many as 150 such audits before December 31, 2012.[1] KPMG auditors will assess whether covered entities have implemented comprehensive policies and procedures that are consistent with the HIPAA rules.[2]

However, even if the possibility of a HIPAA audit is slight, covered entities and business associates should assess their compliance with the privacy and security rules for two reasons: to avoid civil monetary penalties, lawsuits, bad publicity, and other harm resulting from a privacy or security breach; and to meet the security and privacy rules' requirements for ongoing assessment of the organization's compliance. Standards and implementation specifications within HIPAA spell out this duty (see HIPAA Refresher below).

HIPAA Refresher

The privacy rule applies to all protected health information, or PHI; the security rule applies only to PHI in electronic form. The privacy rule is not specific as to standards for protecting PHI. Its Safeguard Implementation Specification, under the Administrative Requirements Standard, requires covered entities reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements of the privacy rule and to reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure (see § 164.530(c)(2)(i) and (ii)).

In addition, the breach notification requirements of the HITECH Act, which modified HIPAA in 2009, require covered entities conduct audits to detect breaches of PHI (see 45 CFR subpart D).

Thus, whether a covered entity or a business associate is ever audited by HHS, these requirements taken together clearly contemplate the covered entity auditing its own compliance. Doing so, of course, would also help the covered entity avoid panic when it received notification of a pending audit.

The following standards and implementation specifications within HIPAA spell out a covered entity's duty to monitor its compliance with the privacy and security rules:

- **Information System Activity Review Implementation Specification under the Security Management Process Standard,** § 164.308(a)(1)(ii)(c). A covered entity must implement procedures to

regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports.

- **Evaluation Standard,** § 164.308(a)(8). The covered entity must perform periodic technical and nontechnical evaluations based initially upon the standards implemented under this rule and subsequently in response to environmental or operational changes affecting the security of electronic PHI. The purpose of these periodic evaluations is to establish the extent to which an entity's security policies and procedures meet the security rule's requirements. Such evaluations may be triggered by changes in technology, business operations, or risk. This standard does not have any implementation specifications. Basically, this standard requires periodic updating of the risk analysis required by the Security Management Process Standard.
- **Audit Controls Standard,** § 164.312(1)(b). Covered entities must implement hardware, software, or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. No implementation specifications augment this standard.
- **Updates under the Policies and Procedures and Documentation Requirements Standard,** § 164.316(b)(2)(iii). Covered entities must review documentation periodically and update as needed in response to environmental or operational changes affecting the security of electronic PHI.

What to Audit

Covered entities can approach an internal compliance audit in two ways. They can audit against a checklist of every relevant HIPAA requirement, or they can focus on those standards and implementation specifications that are key-those items for which noncompliance would likely result in a valid complaint to OCR, a serious breach of protected health information (PHI), a civil monetary penalty, or a criminal indictment.[3]

Regardless of the approach, six areas are critical to adequately assess HIPAA compliance.

Risk Analysis

The first question for a covered entity to answer is whether it has ever performed a formal risk analysis. Risk analysis is the absolute key to HIPAA compliance. Not only is it required under the rule's Security Management Process, but it is how an entity knows whether its security measures are reasonable and appropriate.

If a covered entity implements a security measure without conducting a risk analysis, it is just guessing. A breach resulting from a security measure that was not reasonable and appropriate because of the lack of a risk analysis would seem to be a breach due to willful neglect, which OCR must formally investigate and which may result in the higher civil monetary penalties that OCR cannot waive.

Although the requirement for a risk analysis is spelled out only in the Administrative Safeguards section of the security rule-and hence applies only to electronic PHI-covered entities will benefit from a written risk analysis of paper and other forms of PHI because of the privacy rule's requirement to safeguard all PHI. How is the harm from a breach of confidentiality of a clinical record significantly different if the record is in electronic or paper format?

The Nationwide Rollup Review of privacy and security rule oversight, conducted by HHS's Office of Inspector General in 2011, noted that the risk analysis deficiencies discussed above could result in "inadequate or inconsistently applied security controls, improperly documented security responsibilities, insufficient protection of information technology resources, and inappropriate disclosures of [electronic] PHI."[4]

If the covered entity has conducted a formal risk analysis, the next question is whether the analysis has been updated in compliance with the evaluation standard.

The evaluation standard does not specify how often the covered entity has to update its risk analysis; however, annually-or more often if new risks arise suddenly-would seem appropriate for all but the least risky operations, such as a noncelebrity dental practice.

Completing or updating a risk analysis will be instrumental in determining whether other high-risk areas, such as improper access and loss or corruption of data, are adequately guarded against.

Training

Assessing the entity's training program also is important. Covered entities are required to maintain training programs on both the security and privacy rules.

Training is important for additional reasons. First, how can the entity's workforce be expected to know what to do and what not to do unless they have received training on the rules? Second, training is important because it is highly visible to auditors. Either the covered entity has the required training records or it does not. A breach due to a lack of training would appear to constitute willful neglect.

Access Control

Access control is critical, as UCLA Health System learned in 2011 when it agreed to an $865,000 settlement with OCR over allegations that its employees had accessed celebrity records without authorization. The health system also entered into a corrective action plan as a result of the violations.[5]

In assessing their access controls, covered entities and business associates should focus on whether they have reasonable and appropriate access policies; controlled physical access to workstations, data, media, and equipment; and reasonable and appropriate technical access controls, such as secure passwords.

Security of Portable Media and Equipment and Paper Records

Security of portable media and equipment and even paper records is a high-risk area critical to assess. A review of reported health data breaches involving 500 or more individuals reveals that the majority involved loss or theft of such items.[6]

In addition to the potential harm to patients, the ramifications for the covered entity can be highly damaging. Last year Massachusetts General Hospital agreed to a $1 million settlement with OCR over potential HIPAA violations resulting from paper records lost by an employee on the subway.[7]

Identification, Reporting, and Handling of Breaches

Because HHS has indicated that KPMG's audits will include breach notification, a covered entity's initial audit should include the identification, reporting, and handling of breaches.

HIPAA's stiffest administrative monetary penalty is reserved for breaches due to willful neglect. Properly detecting breaches, taking immediate action to contain them, and taking corrective action, including mitigating the harm of the breach and making required reports to HHS and to the subjects of the breach, are crucial in minimizing harm to the subjects of the breach and to the covered entity.[8]

Implementation and Enforcement of Policies

Finally, the covered entity's internal compliance audit should determine whether it has policies crucial to safeguarding PHI. The only policy that the privacy rule requires is the sanction policy. But the duty to safeguard PHI implies adoption of many other policies besides those specified in the security rule (e.g., access policies, workforce clearance procedure, termination procedure, disaster plan, emergency mode operation plan, and so forth), such as a release of information policy, patient access policy, a work-at-home policy, and more.

OCR is likely to view a breach in an area in which the covered entity did not have a written policy as a breach based on willful neglect.

Notes

1. Department of Health and Human Services, HHS Task Order HHSP233201100252G, Contract GS-3F-8127H, Audit Contract.
2. Greene, Adam H. "HHS Steps up HIPAA Audits: Now is the Time to Review Security Policies and Procedures." *Journal of AHIMA*, 82, no. 10 (Oct. 2011): 58–59.
3. Tomes, Jonathan P. "Auditing for HIPAA Privacy Compliance." *New Perspectives* 22, no. 2 (Spring 2003): 5.
4. Department of Health and Human Services, Office of Inspector General. Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability Act of 1996 Oversight, May 2011, A-04-08-05069. http://oig.hhs.gov.
5. Ornstein, Charles. "UCLA Health System Pays $865,000 to Settle Celebrity Privacy Allegations." July 7, 2011. www.propublica.org/article/ucla-health-system-pays-865000-to-settle-celebrity-privacy-allegations/single.
6. Department of Health and Human Services. "Breaches Affecting 500 or More Individuals." www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.
7. Department of Health and Human Services. "Massachusetts General Hospital Settles Potential HIPAA Violations." February 24, 2011. www.hhs.gov/news/press/2011pres/02/20110224b.html.
8. Tomes, Jonathan. *How to Handle HIPAA and HITECH Act Breaches, Complaints, and Investigations: Everything You Need To Know*. Overland Park, KS: Veterans Press, 2011.

Jonathan P. Tomes (jon@tomesdvorak.com) is a partner at Tomes & Dvorak, Chartered, in Overland Park, KS, and president of EMR Legal, Inc.

Article citation:
Tomes, Jonathan P.. "Keeping It Private: Staying Compliant with the HIPAA Privacy and Security Rules" *Journal of AHIMA* 83, no.3 (March 2012): 32-34.