Oregon Healthcare News

orhcnews.com | Articles, Interviews and Statistics for the Healthcare Executive

Newly Released Protocols Provide Guidance for HIPAA Audit Program

By Casey Moriarty
Attorney
Miller Nash LLP

The 2009 HITECH Act mandated many changes to the HIPAA regulations. One such change requires the Office of Civil Rights ("OCR") of the Department of Health and Human Services to conduct "periodic audits" on covered entities and business associates to ensure HIPAA compliance. OCR's stated goal for the audits is to help covered entities and business associates improve compliance with the HIPAA Privacy and Security Rules. In furtherance of this goal, OCR plans to share best practices for HIPAA compliance that are learned through the Audit Program. No fines will directly result from the HIPAA audits, but OCR could initiate a separate investigation based on the audit findings.

OCR is currently conducting a pilot audit of 150 randomly selected covered entities throughout the country, which OCR anticipates completing by the end of the year. Although the Audit Program is starting with a limited number of entities, the Program is expected to grow in the coming years.

In order to shed light on what covered entities and business associates can expect from a HIPAA audit, OCR released the official Audit Protocols on July 3, 2012. You can view the Protocols at: http://ocrnotifications.hhs.gov/hipaa.html.

The Audit Protocols are divided into two sections: one section for the HIPAA Privacy Rule and one section for the HIPAA Security Rule. There are 88 different protocols for the Privacy Rule and 77 different protocols for the Security Rule. Each protocol is taken directly from the text of the HIPAA regulations. In analyzing the Audit Protocols, covered entities and business associates should focus on the "Audit Procedures" part of each protocol. The Audit Procedures set forth the specific questions, requests, and other inquiries that OCR audit contractors must direct to audited entities. For example, in the "risk assessment" protocol for the HIPAA Security Rule, the Audit Procedures require contractors to "Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of [electronic protected health information]."

Covered entities and business associates should feel prepared for a HIPAA audit if they have policies, procedures, and answers for each of the inquiries and requests in the Audit Procedures. It is, of course, understandable if entities do not have the time and resources to analyze and prepare responses to the 165 different protocols. But here are a few compliance steps that will help covered entities and business associates to prepare for a HIPAA audit.

Privacy Rule:

- Prepare policies for the proper use or disclosure of health information, including disclosures

for treatment, payment, healthcare operations, disclosures under a valid patient authorization, and disclosures under other HIPAA exceptions (disclosures to law enforcement, as required by law, etc.);

- Prepare policies for responding to patient requests for access, amendment, and accounting of disclosures of protected health information;
- Prepare policies for compliance with the Breach Notification Rule of the HITECH Act;
- Review and evaluate compliance with the business associate agreement requirements;
- Ensure that staff members who interact with health information receive adequate training for HIPAA compliance;
- Prepare policies and procedures for ensuring that the "minimum necessary" amount of protected health information is disclosed to accomplish an intended purpose;
- Prepare a "sanction" policy for staff members who violate HIPAA;
- If applicable, ensure that the covered entity's Notice of Privacy Practices is updated.

Security Rule:

- Perform annual risk assessments, preferably with the assistance of a third party, to detect HIPAA compliance vulnerabilities;
- Actively monitor access and use of systems containing protected health information;
- Develop a process to create a unique user name and password when granting access to a workforce member;
- Encrypt protected health information whenever possible;
- Implement "role-based" access to protected health information based on individual roles or job duties, and actively monitor and modify such access;
- When possible, de-identify protected health information before sending it to third parties;
- Implement procedures to properly dispose of health information;
- Create a contingency plan to respond to an emergency that damages systems containing electronic protected health information;
- Back up computer systems offsite to ensure that retrievable exact copies of electronic protected health information are available;
- Ensure that a "Privacy Officer" has been designated for the organization.

This list is not all-inclusive, but acting on these recommendations will help assist entities in responding to a HIPAA audit. Even if OCR does not select your organization for an audit, focusing on HIPAA compliance will reduce the risk of a costly breach of protected health information.

Casey Moriarty is a healthcare attorney at Miller Nash LLP. He can be reached at casey.moriarty@millernash.com or 206.622.8484.

Miller Nash is a multispecialty law firm with over 110 attorneys in offices in Seattle and Vancouver, Washington, and Portland and central Oregon. To learn more about Miller Nash, visit www.millernash.com. To read about new or proposed healthcare legal developments, visit our blog at www.healthlawinsights.com.

Reprinted with permission from the Oregon Healthcare News. To learn more about the Oregon Healthcare News visit orhcnews.com.