HIPAA AUDITS IN TIME FOR THE HOLIDAYS

By: Laurel Van Buskirk, Esq.
Email: lvanbuskirk@devinemillimet.com
Phone: 603.695.8565

November 21, 2011

As we gear up for the madness of the holiday season, certain "covered entities," that fall under the purview of the Health Insurance Portability and Accountability Act ("HIPAA"), can look forward to receiving more than just good natured holiday cards in the mail.

Audit Pilot Program

On November 8, 2011, the Office of Civil Rights ("OCR") of the U.S. Department of Health & Human Services ("HHS") announced that it will launch a pilot program to audit providers for compliance with the HIPAA Privacy and Security Rules and Breach Notification standards.[1] The HIPAA Privacy Rule[2] concerns protected health information ("PHI")[3], while the HIPAA Security Standard applies to electronic protected health information ("ePHI")[4] transmitted or maintained in electronic form.

By law, HHS is required to provide for periodic audits to ensure that covered entities and Business Associates are complying with these standards.[5] To implement this mandate, OCR is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance. OCR expects that the audit will include a wide range of types and sizes of covered entities, covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses. Business Associates are not included in the pilot program, but they will be included in future audits. This pilot audit program will begin November 2011 and end by December 2012.

Selected Covered Entities

OCR will notify in writing covered entities selected for an audit and ask them to provide documentation of their privacy and security compliance

[1]For a detailed summary of the HIPAA Privacy & Security Audit Program, *see* U.S. Department of Health and Human Services, HIPAA Privacy & Security Audit Program, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

[2]The HIPAA Privacy Rule is located at 45 C.F.R. Part 160 and Subparts A and E of Part 164.

[3]*See* 45 C.F.R. 164.501.

[4]*See* 45 C.F.R. 164.302.

[5]*See* 42 U.S.C. § 17940.

Office Locations:

111 Amherst Street
Manchester, NH 03101
T 603.669.1000
F 603.669.8547

43 North Main Street
Concord, NH 03301
T 603.226.1000
F 603.226.1001

efforts. Selected covered entities will also be subject to a site visit. As with most government audit processes, during the site visit, auditors will interview key personnel and observe processes and operations to help determine compliance. After completion of the site visit, auditors will develop and issue a draft report describing how the audit was conducted, the findings of the audit, and any corrective action taken as a result of the audit.

Purpose of HIPAA Privacy & Security Audits

This audit pilot program will allow OCR to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews. OCR will also broadly share best practices gleaned through the audit process and guide covered entities in the future.

According to the webpage devoted to the audit program, OCR states that it presently views the pilot audits as primarily a compliance improvement tool, rather than an enforcement tool. That said, new HHS Director, Leon Rodriguez, has previously commented that he believes in both aggressive HIPAA enforcement as well as compliance education. In an interview, Rodriguez stated, "As I've learned as a prosecutor and then as a defense lawyer, enforcement promotes compliance. The fact that covered entities out there know that they are at risk for penalties is something that, in fact, in many cases will promote compliance."[6] Rodriguez recognizes the importance of educating and assisting covered entities in understanding the rules and regulations.

Penalties

Penalties for failure to comply with requirements and standards of HIPAA may range from $100 per violation to $50,000 or more per violation, depending on the circumstances of the violation.[7] Aggregate penalties for multiple violations of the same requirement are capped for each calendar year at $1,500,000 for violations occurring on or after February 18, 2009 or $25,000 for violations occurring before February 18, 2009.[8]

The amount of the penalty depends on: the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect.[9] While OCR may impose civil monetary penalties on covered entities for a failure to comply, it generally will not do so if the failure to comply was not due to willful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred.[10] This means that audited covered entities that previously had been unaware of an issue of non-compliance will likely have a grace period in which to fix any compliance concerns found during the audit process.

---

[6] HealthCare Information Security, "New HIPAA Enforcer Pinpoints Priorities," http://www.healthcareinfosecurity.com/articles.php?art_id=4153.

[7] *See* 42 U.S.C. § 1320d-5(a).

[8] *See* 42 U.S.C. § 1320d-5(a)(3)(D).

[9] *See* 42 U.S.C. § 1320d-5(a).

[10] *See* 42 U.S.C. § 1320d-5(b)(2)(A).

Entities with known, long standing violations, on the other hand, can expect to be penalized.

HIPAA violations may also result in criminal penalties of up to $50,000 and up to one-year imprisonment.[11] Criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm.[12] Criminal prosecutions are handled by the Department of Justice.

In addition, under the Health Information Technology for Clinical and Economic Health (HITECH) Act, state attorneys general are empowered to bring civil lawsuits against covered entities and business associates that commit HIPAA violations that injure citizens in their state.[13] Currently, OCR is offering HIPAA Enforcement Training to help State Attorney Generals and their staff use their new authority to enforce the HIPAA Privacy and Security Rules, which includes training to aid State Attorneys General in investigating and seeking damages for HIPAA violations that affect residents of their states.

Recommendations for Covered Entities

While the HHS's announcement has caused understandable concern among covered entities, the reality is that only a statistically small number of covered entities will be affected nationally. With that being said, given the severity of civil and criminal penalties, combined with the vocalized intention of the new HHS Director to aggressively enforce compliance going forward, all covered entities should assume they are at risk and take the necessary precautionary steps to ensure HIPAA compliance.

It would be prudent for all covered entities to take the following action: (1) Review HIPAA policies and procedures to ensure they are up-to-date; (2) Train employees on the policies and the importance of consistent adherence; (3) Educate employees on the consequences for non-compliance; and (4) Adopt a prompt action plan to respond to incidents.

The Devine, Millimet & Branch Healthcare Practice offers this free periodic E-Mail Alert service to provide information on recent healthcare developments in statutory, regulatory and case law, and decisions. If you have any questions about this e-mail, or if you know of anyone else who may be interested in receiving these alerts, please send us an e-mail at *healthcare@devinemillimet.com*.

[11] *See* 42 U.S.C. § 1320d-6.

[12] *See id.*

[13] *See* 42 U.S.C. § 1320d-5(d).