Health Law Alert: OIG Audit Exposes Vulnerabilities in HIPAA Security Rule Compliance, Offers Lessons for Covered Entities and Business Associates

June 2, 2011

On May 16, 2011, the Department of Health & Human Services (HHS) Office of Inspector General (OIG) released an audit report discussing vulnerabilities in the policies and procedures used by Covered Entities to safeguard the confidentiality, integrity, and availability of electronic protected health information (ePHI). The report is intended to assess the sufficiency of the Centers for Medicare & Medicaid Services (CMS)' oversight of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The OIG's report, which discusses specific compliance issues discovered at the Covered Entities that were audited, offers insight into what is required to successfully implement the technical, administrative, and physical safeguards mandated under the Security Rule.

The report should also help Business Associates of Covered Entities in understanding the obligations to which they will soon be subject under the Security Rule, as a result of changes from 2009's Health Information Technology for Economic and Clinical Health Act (HITECH). Regulations proposed last summer (73 Fed. Reg. 40868, Jul. 14, 2010) implementing the Security Rule's application to Business Associates have not yet been finalized. Given the complexity of complying with the Security Rule, many organizations—historically regulated only through Business Associate Agreements with Covered Entities—are struggling to understand what implementing the safeguards required under the Security Rule truly means.

Audit of CMS' Oversight and Enforcement of the HIPAA Security Rule

The OIG's report is based on an audit of hospitals it conducted to evaluate the effectiveness of their efforts to comply with the Security Rule. The report identifies numerous internal control weaknesses at the hospitals and concludes that the Office for Civil Rights (OCR) should engage in enhanced oversight of compliance with the Security Rule.

At the hospitals audited, the OIG identified 151 vulnerabilities in the systems and controls intended to protect ePHI. Of these vulnerabilities, 124 were categorized as high impact, meaning that they may result in the costly loss of major tangible assets, may significantly violate or harm an organization's mission, or may result in serious injury or human death. The weaknesses identified at the hospitals included:

- ***Wireless Access Vulnerabilities***: The OIG noted that several of the Covered Entities used ineffective encryption and failed to ensure authentication as a condition of users entering the hospital's wireless network. In addition, the OIG discovered hospitals that did not have the ability to detect unauthorized devices accessing the wireless network.
- ***Access Control Vulnerabilities***: These included inadequate password settings, computers that did not automatically log users off after periods of inactivity, and unencrypted laptops containing ePHI. The OIG discussed hospitals that failed to require that passwords be changed periodically or have a minimum number of characters.
- ***Audit Control Vulnerabilities***: The OIG noted Covered Entities that had disabled available audit logging. In addition, the network administrators at several hospitals failed to engage in the regular review of audit logs, either manually or through automated log-monitoring tools.
- ***Integrity Control Vulnerabilities***: The OIG discussed the failure to install security patches, the use of outdated antivirus updates, and hospitals allowing unrestricted Internet access, including permitting personnel to download and install software to network computers without sufficient internal oversight.
- ***Person or Entity Authentication Vulnerabilities***: Weaknesses mentioned by the OIG included inappropriate sharing of system administrator accounts and unchanged default user identifiers and passwords. The OIG noted that many default passwords are available on the Internet and in online software user manuals.
- ***Facility Access Control Vulnerabilities***: The OIG mentioned unsecured physical access to ePHI in data centers. In addition, the OIG described large open shelves and unlocked windows, which creates a danger of ePHI being exposed to unauthorized personnel.
- ***Device and Media Control Vulnerabilities***: The problems noted by the OIG included lack of inventory systems to track computer equipment containing ePHI, no documented plans for or evidence of removal of ePHI before disposal, no password protection for computers, and no encryption on software backups containing ePHI.
- ***Security Management Process Vulnerabilities***: Problems included incomplete risk assessments and lack of policies and procedures for risk analysis. This creates a compliance issue because the goal of the risk assessment is for Covered Entities to engage in a thorough internal analysis of weaknesses in their approach to data security, so as to permit the Entity to take informed steps to address those weaknesses.
- ***Workforce Security Vulnerabilities***: The OIG discovered Covered Entities whose employee user accounts allowed for inappropriate network access. The OIG also noted hospitals that failed to deactivate terminated employees' network access, thereby allowing these former employees to continue accessing ePHI after their departure.
- ***Security Incident Procedure Vulnerabilities***: The issues discussed by OIG included lack of procedures to identify, respond to, or document actions taken in response to security incidents. The OIG discussed a hospital that failed to confiscate a laptop computer for inspection for three days after a security incident was reported to the hospital.
- ***Contingency Plan Vulnerabilities***: Issues included incomplete contingency plans, incomplete disaster recovery plans, unsafe storage of backup tapes, and network security disruptions. The OIG discussed a hospital that did not have any contingency plan for a system that provided access to patient health care

records and test results, which created a risk that ePHI would not be available in the event of a system crash.

HIPAA Oversight and Enforcement on the Rise

The OIG concluded that oversight and enforcement have been insufficient as a means of ensuring that Covered Entities comply with the Security Rule. With increased penalties for noncompliance and greater public awareness about HIPAA, oversight of Covered Entities and Business Associates' compliance will continue to be an area of focus for regulators. Meanwhile, HHS has not yet indicated when the proposed HITECH regulations will be finalized.

HIPAA and HITECH issues will be a key topic at Gray Plant Mooty's 15th Annual Health Law Conference, to be held July 14, 2011, at the Earle Brown Heritage Center in Brooklyn Center, Minnesota. This event is free. An invitation and registration information will follow in June. If you have any questions, please contact events@lathropgpm.com.

If you have questions about the OIG report or the HIPAA Security Rule, please contact Jesse Berg at 612.632.3374 or jesse.berg@lathropgpm.com.