Connecting Healthcare with Legal Excellence℠

Health Law Diagnosis

HIPAA AUDITS SCHEDULED TO BEGIN NOVEMBER 2011

The United States Department of Health and Human Services (HHS) has announced that it will begin HIPAA audits of covered entities and business associates this November 2011, and its contracted auditor, KPMG, is required to audit up to 150 entities by the end of 2012! HHS's website provides detailed information regarding ***when*** the audits will begin, ***who*** may be audited, ***how*** the audit program will work, ***what*** the general timeline will be for an audit, and, generally, ***what*** will happen after an audit is completed (*see* **www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html**). In addition, the sample **HHS Audit Letter** posted on its website indicates that KPMG will focus on discovering vulnerabilities in privacy and security compliance programs, and that certain "information" and "documents" will be requested in connection with the audit. However, no additional details are given regarding what covered entities and business associates may be asked to produce.

Presumably, KPMG will not be letting the HIPAA audit cat out of the bag too soon by telling organizations exactly what information and documents they may ask for in connection with such audits, especially where one of their objectives is to identify gaps in HIPAA compliance. Nevertheless, covered entities and business associates may gain valuable insight into what to expect by looking to past guidance regarding HIPAA audits issued by HSS's Office of e-Health Standards and Services (the "**HIPAA Audit Checklist**"), as well as by reviewing HIPAA audits and investigations that have taken place over the last few years.

In its formerly-released **HIPAA Audit Checklist,** the Office of e-Health told us the following:

- **Personnel that may be interviewed**
  - President, CEO or Director
  - HIPAA Compliance Officer
  - Lead Systems Manager or Director
  - Systems Security Officer
  - Lead Network Engineer and/or individuals responsible for:
    - administration of systems which store, transmit, or access e-PHI
    - administration systems networks (wired and wireless)
    - monitoring of systems which store, transmit, or access e-PHI
    - monitoring systems networks (if different from above)
  - Computer Hardware Specialist
  - Disaster Recovery Specialist or person in charge of data backup
  - Facility Access Control Coordinator (physical security)
  - Human Resources Representative
  - Director of Training
  - Incident Response Team Leader
  - Others as identified….

- ***Policies** and **Procedures and other evidence** that address the following may be requested*:
  - ☐ Prevention, detection, containment, and correction of security violations
  - ☐ Employee background checks and confidentiality agreements
  - ☐ Establishing user access for new and existing employees
  - ☐ List of authentication methods used to identify users authorized to access e-PHI
  - ☐ List of individuals and contractors with access to e-PHI, and include copies pertinent business associate agreements
  - ☐ List of software used to manage and control access to the Internet
  - ☐ Detecting, reporting, and responding to security incidents (if not in the security plan)
  - ☐ Physical security
  - ☐ Encryption and decryption of e-PHI
  - ☐ Mechanisms to ensure integrity of data during transmission - including portable media transmission (i.e. laptops, cell phones, blackberries, thumb drives)
  - ☐ Monitoring systems use - authorized and unauthorized
  - ☐ Use of wireless networks
  - ☐ Granting, approving, and monitoring systems access (e.g., by level, role, and job function)
  - ☐ Sanctions for workforce in violation of policies/procedures governing e-PHI access or use
  - ☐ Termination of systems access by workforce (and others granted access)
  - ☐ Session termination policies and procedures for inactive computers
  - ☐ Policies and procedures for emergency access to electronic information systems
  - ☐ Password management policies and procedures
  - ☐ Secure workstation use (documentation of specific guidelines for each class of workstation (i.e., on site, laptop, and home system usage)
  - ☐ Disposal of media and devices containing e-PHI
- ***Other Documents that may be requested:***
  - ☐ Entity-wide Security Plan
  - ☐ Risk Analysis (most recent)
  - ☐ Risk Management Plan (addressing risks identified in the Risk Analysis)
  - ☐ Security violation monitoring reports
  - ☐ Vulnerability scanning plans (results from most recent vulnerability scan)
  - ☐ Network penetration testing policy/procedure (results from most recent penetration test)
  - ☐ List of all user accounts with access to systems which store, transmit, or access e-PHI (for active and terminated employees)
  - ☐ Configuration standards to include patch management for systems which store, transmit, or access e-PHI (including workstations)
  - ☐ Encryption or equivalent measures implemented on systems that store, transmit, or access e-PHI
  - ☐ Organization chart to include staff members responsible for general HIPAA compliance
  - ☐ Documentation of training delivered to staff members to ensure awareness and understanding of e-PHI policies and procedures (security awareness training)
  - ☐ Policies and procedures governing the use of virus protection software
  - ☐ Data backup procedures
  - ☐ Disaster recovery plan
  - ☐ Disaster recovery test plans and results
  - ☐ Analysis of info systems, applications, data groups according to their criticality and sensitivity
  - ☐ Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit or maintain e-PHI
  - ☐ List of all Primary Domain Controllers (PDC) and servers
  - ☐ Inventory log recording the owner and movement media and devices that contain e-PHI

One case that is particularly informative is the audit of Atlanta, Georgia's Piedmont Hospital (the "**Piedmont Audit**"). In February of 2007, HHS through the Office of Inspector General conducted a random HIPAA audit of Piedmont hospital. The letter to Piedmont's CIO announced that the focus of the audit would be on the organization's compliance with the Security Rule and indicated that the audit would begin with an "entrance conference" 10 days after Piedmont's receipt of the audit letter from the Regional Inspector General for Audit Services (note that the proposed timeframe for coming KPMG audits is *30-90 calendar days* from the date on the applicable HHS Audit Letter). The Piedmont audit letter also included an enclosure asking for a list of documents and information to be provided, which overlapped significantly with the Office of e-Health's HIPAA Audit Checklist. Specifically, the Piedmont letter asked for the following:

- **Policies** and **Procedures** regarding:
  - establishing and terminating users' access to systems housing e-PHI
  - emergency access to electronic information systems
  - inactive computer sessions ("timeout" after period of inactivity)
  - recording and examining activity in info systems that contain or use e-PHI (i.e., audit trails)
  - risk assessments and analyses of relevant info systems that house or process e-PHI
  - sanctions imposed for employee violations
  - electronic transmission of e-PHI
  - preventing, detecting, containing, correcting security violations (i.e., incident reports)
  - regularly reviewing records of information system activity, such as audit logs, access reports, and security incident tracking reports
  - creating, documenting, and reviewing exception reports or logs (Piedmont was asked to provide a list or examples of security violation logging and monitoring)
  - monitoring systems and the network, including a listing of all network perimeter devices (i.e., firewalls and router)
  - physical access to electronic information systems and the facility in which they are housed
  - establishing security access controls (what types of security access controls are currently implemented or installed in the covered entity's/business associate's database that houses e-PHI?)
  - remote access activity (i.e., network infrastructure, platform, access servers, authentication, and encryption software)
  - internet usage
  - wireless security (transmission and usage)
  - firewalls, routers, and switches
  - maintenance and repairs of hardware, walls, doors, and locks in sensitive areas
  - terminating an electronic session and encrypting and decrypting e-PHI
  - transmitting e-PHI
  - passwords and server configurations
  - antivirus software
  - network remote access
  - computer patch management

- In addition, other documentation specifically requested included:
  - list of all information systems that house e-PHI data, as well as network diagrams, including all hardware and software used to collect, store, process, or transmit e-PHI
  - list of terminated employees
  - list of all new hires
  - list of encryption mechanisms used for e-PHI
  - list of authentication methods used to identify users authorized to access e-PHI

- list of all outsourced individuals and contractors with access to e-PHI data, if applicable, and a copy of the contract for each of these individuals/contractors
- list of transmission methods used to transmit e-PHI over an electronic communications network
- organizational charts that include names and titles for the management (i.e., information system and information system security departments)
- an entity-wide security program plan (e.g., System Security Plan)
- list of all users with access to e-PHI data, and the defined scope of each such user's access rights and privileges
- list of system administrators, backup operators, and users
- list of antivirus servers installed, including their versions
- list of software used to manage and control access to the Internet
- identify the antivirus software used for desktop and other devices, including their versions
- list of all users with remote access capabilities
- list of database security requirements and settings
- list of all PDC and servers (including UNIX, Apple, Linx, and Windows), and identify whether these servers are used for processing, maintenance, updating, and storing e-PHI
- listing of authentication approaches used to verify a person has been authorized for specific access privileges to information and information systems

In addition to the Piedmont Audit, covered entities and business associates may glean additional insight from what HHS/OCR has asked for in connection with complaint-driven HIPAA investigations. HHS/OCR has posted on its website **several Resolution Agreements** with covered entities who have been through a HIPAA investigation. These agreements also contain hints as to what covered entities and business associates may be asked for during a HIPAA Audit.

Until news of organizations starting to receive HIPAA audit letters starts to trickle out and KPMG begins its work, it is not possible to know exactly what KPMG will ask for and focus on. Nevertheless, covered entities and business associates should not sit back and take a "wait and see" approach. Rather, organizations should prepare now by completing an internal review of their HIPAA compliance program to ensure that their policies are current and are being followed by their workforce, and all other required HIPAA documentation is in place and ready to be produced in case a HIPAA Audit letter arrives in the mailbox tomorrow.

* * * *

For more information, please contact:

Helen Oscislawski, Esq.
Principal at Oscislawski LLC
tel: 609-385-0833, ext. 1
helen@oscislaw.com

OR

Krystyna Monticello, Esq.
Partner at Oscislawski LLC
tel: 609-385-0833, ext. 2
kmonticello@oscislaw.com

Attorneys at Oscislawski LLC is a health law firm with its main office located in Princeton, New Jersey but a nationwide reputation for experience with and understanding of federal and state privacy and security laws, as well as electronic health information exchange, health information technology, and managing health data breaches. Our attorneys also advise clients on wide-range of other legal issues. For more information about our firm visit www.oscislaw.com. ***For excellent compliance information, tools and solutions, please also visit our affiliated blog & resource website*** *www.legalhie.com.*