Davis Wright Tremaine LLP

HHS Audits the 1% … and the Rest: First HIPAA Privacy and Security Audits Begin

By Adam H. Greene

December 13, 2011

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has begun the process of notifying covered entities that they are among the unlucky few who have been selected for the first Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security audits under the Health Information Technology for Economic and Clinical Health (HITECH) Act. The selected entities represent a cross sample of the health care industry—from billion-dollar health care systems to small physician practices. Audited entities will undergo comprehensive reviews of their privacy and security policies and procedures, documentation, and operations.

While the first twenty covered entities have been selected, approximately another 130 remain in this audit round. HHS has indicated that it hopes to continue with proactive audits in the future and expects to become more aggressive in its enforcement of complaints. Accordingly, now is a good time to ensure that:

- Policies, procedures, and documentation comprehensively address all privacy and security requirements;
- Privacy and security training has been completed and documented;
- Actions taken as part of the HIPAA compliance program has been documented, such as complaints and any resulting investigations, findings, and mitigation; and
- Your security risk assessment and documentation of your risk management decision-making process are up to date.

The Unlucky Winners

HHS divided the covered entity population into four levels and various types of covered entities.

Level 1 Entities Large providers/payors with more than $1 billion in revenue and/or assets	**Level 2 Entities** Large regional hospital systems/Regional payor with between $300 million and $1 billion in revenue and/or assets
Level 3 Entities Community hospitals, ambulatory surgery centers, regional pharmacies (with between $50 million and $300 million in revenue and/or assets) and self-insured entities that do not adjudicate their claims	**Level 4 Entities** Small providers and community pharmacies with less than $50 million in revenue and/or assets

Covered Entity Type	Level 1	Level 2	Level 3	Level 4	Total
Health plans	2	3	1	2	8
Health care providers	2	2	2	4	10
Health care clearinghouses	1	1	0	0	2
Total	5	6	3	6	20

Health Plans	
Medicaid	1
SCHIP	1
Group Health Plans	3
Health Insurance Issuer	3
Total	8

Health Care Providers	
Allopathic & Osteopathic Physicians	3
Hospitals	3
Laboratories	1
Dental	1
Nursing and Custodial Facilities	1
Pharmacy	1
Total	10

The audit notification letters have gone out to the above health plans, hospitals, pharmacies, health care clearinghouses, and small practices. Site visits are expected to begin in mid-January.

What Audited Entities Can Expect

We anticipate that the selected covered entities received notification letters, coupled with requests for documentation. These covered entities may have as little as ten business days to respond. The requested information may include policies and procedures, training materials and documentation, a security risk analysis, and other documentation required by the HIPAA regulations.

The site visits, which likely will begin next month, will include a team of auditors spending between three and ten business days on site, interviewing leadership and inspecting the premises. The auditors may review administrative, physical, and technical safeguards of written, oral, and electronic protected health information.

How to Prepare

The audits represent a good opportunity to take stock of your privacy and security programs and make improvements. OCR has indicated that, after publication of final rules modifying the HIPAA regulations in accordance with the HITECH Act, they will more aggressively pursue complaints where there are indications of noncompliance due to willful neglect. Preparing for the current wave of HIPAA audits will help prepare your organization for this heightened enforcement.

A few steps that your organization can take to help prepare for audits include:

- Addressing the entire lifecycle of electronic and hard copy protected health information, identifying where such information is created throughout the organization, how it is maintained, and how it is disposed of;
- Creating a compliance cycle that regularly modifies policies and training in response to recurring issues and emerging threats; and
- Conducting a comprehensive review of policies, procedures, other documentation, and training.