Davis Wright Tremaine LLP

Turning Up the Heat: OIG Reports Highlight Security Vulnerabilities and Lack of HHS Oversight

By Adam H. Greene* and Rebecca L. Williams

May 19, 2011

On May 16, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) issued two reports critical of the HHS' efforts to ensure the security of electronic health information. The first report criticized the Centers for Medicare & Medicaid Services (CMS) for its prior oversight of the HIPAA Security Rule. The second report criticized the Office of the National Coordinator for Health Information Technology (ONC) for insufficiently building security into the requirements for certified electronic health records.

These reports demonstrate that there is significant pressure on ONC, the Office for Civil Rights (OCR), and CMS to build more stringent security controls into health information technology (IT) systems, and that a number of specific vulnerabilities have been highlighted. Covered entities and business associates may be well served to use these reports to proactively assess their own systems for these high-impact vulnerabilities. We provide a vulnerability checklist at the end of this alert to assist organizations in conducting their own risk analyses.

OIG criticizes lack of government oversight

Privacy advocates, the HIT Policy Committee's Privacy and Security Tiger Team, and members of Congress already have expressed concern with HHS over a perceived lack of emphasis on health information security. These two reports add another voice, this time from HHS' own watchdog, to this chorus. They also provide the health care community with information about potential vulnerabilities and raise the probability of heightened HIPAA security enforcement (such as through the upcoming audit program) and more stringent security requirements for electronic health records.

The OIG's report on oversight of the HIPAA Security Rule concluded that CMS' oversight and enforcement actions were insufficient to ensure that covered entities, such as hospitals, physician practices, and health plans, effectively implemented the Security Rule, leaving electronic protected health information (ePHI) vulnerable to attack and compromise.

After auditing seven hospitals located across the country, the OIG identified 151 vulnerabilities in systems and controls intended to protect ePHI, of which the OIG categorized 124 vulnerabilities as high impact. The identified high-impact vulnerabilities included problems with technical safeguards (wireless network access, access control, audit control, integrity control, authentication, and transmission security), physical safeguards (facility access and device and media control), and administrative safeguards (security management, workforce security, security incident procedures, and contingency planning).

OIG calls for proactive compliance audits

The OIG's recommendation is for OCR, which now has authority for enforcement of the Security Rule, to continue CMS' most recent efforts by conducting proactive compliance reviews (rather than launching investigations based only on complaints or media reports). The OIG's recommendation also is consistent with the mandate for proactive audits under the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). OCR is in the process of launching an audit program pursuant to a requirement of the HITECH Act. Based on recent OCR statements, a pilot audit program is expected later this year. The OIG recommendation begs the question of whether the vulnerabilities identified by the OIG will be included in OCR's upcoming audit efforts.

OIG recommends expanded EHR security standards

The OIG's report on ONC's security effort primarily focused on the standards and certification criteria for electronic health records (EHRs). After reviewing these standards, which ONC promulgated as part of the meaningful use program, the OIG criticized ONC for including only application-specific IT security standards, rather than general IT security standards. The OIG expressed concern that application-specific security controls can be bypassed due to a lack of general security controls.

For example, while ONC's standards address encryption of transmissions between systems, the OIG criticized ONC for not including standards requiring encryption of data stored on mobile devices, two-factor authentication for systems containing electronic health information, and the regular updating of operating systems. The report recommends that ONC broaden its standards to include general IT security controls, use its leadership role to promote IT security best practices, emphasize to the health care community the importance of general IT security, and coordinate with CMS and OCR.

The OIG report on ONC's security efforts appears to miss the mark in one significant way. ONC's EHR standards are the foundation of ONC's certification program for EHR software. During this process, ONC-authorized testing and certification bodies review EHR software to ensure that it satisfies ONC's standards. Because the certification process is limited to EHR software (it does not evaluate the general IT environment where the EHR technology would be installed), it is unclear how the certification bodies could certify general IT controls as recommended by the OIG.

Checklist: security risks

The following is a detailed checklist of these vulnerabilities to assist covered entities and business associates with assessing their own systems for the identified high-impact vulnerabilities.

Identified Vulnerability	Addressed?
Wireless Access	
Ineffective encryption	
No firewall separating wireless from wired network	
Broadcasted service set identifiers (SSIDs) from access points (allowing unauthorized users to identify and potentially access the network)	
No authentication required to access wireless network	
Inability to detect devices intruding on the wireless network	
No procedure for continuously monitoring the wireless network	
Access Control	
Inadequate password settings	
No auto-logoff after period of inactivity	
Unencrypted laptops containing ePHI	
Excessive access to root folders	
Audit Control	
Audit logging disabled	
Failure to review operating system and application audit logs (manually or through automatic tools)	
Integrity Control	
Uninstalled critical security patches	
Outdated antivirus updates	
Operating systems no longer supported by manufacturer	
Unrestricted Internet access	
Person or Entity Authentication	
Inappropriate sharing of administrator accounts	
Unchanged default user identifiers and passwords	
Transmission Security	
Inappropriate plain text remote administration tools (e.g., Simple Network Management Protocol version 1 and the Telnet protocol)	
No email encryption	
Unsecure switch port connections	
Unnecessary and unsecure network services	
Facility Access Control	
Unsecured access to data center and backup room	
Device and Media Controls	
No inventory system tracking computers containing ePHI	

No documented plan for or evidence of removal of ePHI from media before disposal	
No password protection for computers on portable carts	
No encryption of backup tapes containing ePHI	
Security Management Process	
Incomplete risk assessment of systems that create, receive, maintain, or transmit ePHI	
No policies or procedures for risk analysis	
Workforce Security	
Employee accounts with inappropriate levels of access to network and ePHI	
Failure to timely terminate user accounts after employee termination	
Security Incident Procedures	
Lack of procedures to identify, respond to, or document actions taken in response to security incidents	
Contingency Plan	
Incomplete contingency plan	
Incomplete disaster recovery plan	
Unsafe storage of backup tapes	

* Davis Wright Tremaine welcomes Adam Greene to our health information technology/HIPAA practice. Adam comes to us from the federal Office for Civil Rights. He is a 12-year health law veteran and was a key regulator at the U.S. Department of Health and Human Services agency responsible for HIPAA enforcement. For more information on Adam, please see our press release.

This advisory is a publication of Davis Wright Tremaine LLP. Our purpose in publishing this advisory is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.