Washington Healthcare News®

wahcnews.com

Articles, Interviews and Statistics for the Healthcare Executive

VOLUME 5, ISSUE 8 AUGUST 2010

Data Security Remains Key Risk Management Issue for Insurers and Other Large Holders of PHI

By Anthony R. Miles
Partner
Stoel Rives LLP

With all the discussion about this year's federal healthcare legislation, HIPAA Security compliance issues may seem like old news. Nonetheless, the list of substantial breach notifications posted on the website of the Department of Health and Human Services (HHS), Office of Civil Rights (OCR), along with developments in HIPAA enforcement and changes to NIST standards, demonstrates that securing protected health information (PHI) remains a worthy focus of risk-management resources for insurance entities, hospitals and health systems, and other organizations with large volumes of PHI.

Last year's Health Information Technology for Economic and Clinical Health Act (HITECH) initiated a sea change in the enforcement of privacy and security protections for PHI under the HIPAA. Under HITECH, covered entities and business associates must report data breaches involving 500 or more unique individuals to HHS. HHS publishes these breaches on its website and has stated that it will investigate all such reports.[i] A review of the current list of reported breaches reveals that a substantial percentage of the nearly 100 such events were reported by health plans (e.g., insurers, either for themselves or as business associates of employer plans, and public agencies) or hospitals and health systems. HITECH grants HHS the authority to impose penalties for violations under almost any circumstances, which makes it all the more surprising that many of these reports could have been avoided with better security technology or improvements in policies, procedures and training.

Fortunately for entities with large volumes of PHI, OCR has indicated that it will continue to use enforcement discretion where appropriate. For example, a covered entity can assert an affirmative defense if the violation was not due to willful neglect and was corrected within 30 days of when it was or should have been discovered.[ii] HHS also retains the discretion to resolve "indications of noncompliance" by informal means and to enter into "Resolution Agreements" to involve indications of violations.[iii] A Resolution Agreement generally includes payment of a resolution amount and incorporates a corrective action plan involving oversight of compliance by HHS including approval of policies and procedures, improved training and other monitoring of implementation and compliance, usually for a period of three years.

HHS takes the position that the resolution amount is not a civil monetary penalty, fine or other penalty, and that its informal processes are not subject oversight by an administrative law judge or other process, so neither is a "get out of jail free" card. An organization entering into a Resolution Agreement must agree to extend the statute of limitations beyond the termination of the Resolution Agreement if it otherwise would expire during

that term of the agreement. This effectively leaves the organization vulnerable to penalties for any underlying noncompliance with the Privacy or Security Rules if the organization does not comply with the terms of the Resolution Agreement.

Under these circumstances, the number of breaches involving more than 500 individuals reported to HHS involving laptops and other portable data storage devices is surprising and suggests that employee mobility and remote access continue to be significant security challenges for organizations that maintain large volumes of health data. Our experience advising clients in data breach scenarios confirms this perspective and suggests other areas in which organizations could further reduce potential exposure to substantial breaches and subsequent enforcement by reviewing their security posture, such as:

- Off-site data storage and data destruction vendors
- Software updates and security patches
- IT Help Desk personnel and procedures
- "Data at rest but in motion"—mobile devices, portable storage media, social networking

Those organizations that have implemented, or are contemplating implementing encryption technology to take advantage of the safe harbor under the Breach Notification Rule[iv] also should note that some of the algorithms originally approved for compliance with the standards set forth in the HHS 2009 Guidance[v] no longer will be approved as part of an overall increase in security strength requirements scheduled for 2011.[vi] Unless HHS issues new guidance overriding the transition schedule for purposes of HIPAA compliance, organizations using encryption modules based on either algorithms with a security strength below 112 bits will need to upgrade their technology prior to January 1, 2011.

Those considering investing in encryption technology should ensure that the products they are considering include technology that will comply with the increased security strength requirements for validation under applicable publications from the National Institute for Standards in Technology (NIST) and Federal Information Processing Standard 140-2. Failure to do so could result in unanticipated interoperability problems with some systems (e.g., community EHRs, ePrescription programs); however, most importantly, interception of a transmission or unauthorized ac-

cess to data encrypted with these technologies may well be the next wave of unexpected notification and reporting responsibilities, and possibly additional enforcement action by HHS.

Tony Miles is a Partner at Stoel Rives LLP who focuses his healthcare practice at the intersection of healthcare regulation and technology. He counsels providers and other health industry in corporate matters, strategic affiliations, technology development and services transactions, and data privacy and security issues involving health information technology. Contact Tony at 206.386.7577 or armiles@stoel.com.

This column is not to be considered legal advice or a legal opinion on specific facts or circumstances. The contents are intended for informational purposes only. If you need legal advice or a legal opinion, please consult with an attorney.

***

[i]David Holtzman, "*How OCR Enforces the Security Rule*," Presentation at NIST, HHS Office of Civil Rights Joint Conference: Safeguarding Health Information: Building Assurance Through HIPAA Security, Washington D.C., May 11, 2010 <available at http://csrc.nist.gov/news_events/HIPAA-May2010_workshop/presentations.html> (last visited June 11, 2010).

[ii]45 C.F.R. § 164.410, 74 Fed. Reg. 56123, 56131 (Oct. 30, 2009).

[iii]45 C.F.R. § 160.312.

[iv]See 45 C.F.R. 164.402 (definition of "Unsecured PHI").

[v]Guidance Specifying Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable or indecipherable to Unauthorized Individuals, 74 Fed. Reg. 19006, 19009 (Apr. 27, 2009).

[vi]See Matthew Scholl, "*NIST and US Civilian Agency Cryptography*," Presentation at NIST, HHS Office of Civil Rights Joint Conference: Safeguarding Health Information: Building Assurance Through HIPAA Security, Washington D.C., May 12, 2010 <available at http://csrc.nist.gov/news_events/HIPAA-May2010_workshop/presentations.html> (last visited June 11, 2010).