Washington Healthcare News®

wahcnews.com

Articles, Interviews and Statistics for the Healthcare Executive

Protecting Patient Data in the Cloud: Understanding New HIPAA Compliance Requirements

By Chris Kradjan
Partner
Moss Adams LLP

By Kevin Villanueva
Senior Manager, IT Consulting Practice
Moss Adams LLP

In January 2013 the Department of Health and Human Services (HHS) finalized the Health Insurance Portability and Accountability Act (HIPAA) omnibus rule, a set of new regulations and changes to existing HIPAA rules designed to preserve patients' privacy regardless of where protected health information (PHI) is being handled.

By holding health care facilities and health IT companies responsible for how they process, store, and disseminate patient data, the final HIPAA omnibus rule strengthens patient privacy protections and establishes new patient rights regarding their PHI. While the rule is an achievement for patient rights, it increases the level and scope of responsibility on providers that manage PHI.

PROVISIONS OF THE FINAL OMNIBUS RULE

Health care facilities should understand the new changes and take appropriate measures to maintain HIPAA compliance. The four areas that have the biggest impact on health care facilities as a result of the final HIPAA omnibus rule are:

- **Modifications to the HIPAA Privacy, Security, and Enforcement Rules.** Business associates—not just covered entities—are now liable for compliance with certain HIPAA Privacy and Security Rules.
- **New Breach Notification Rule.** The definition of *breach* is expanded to include the risk of impermissible use or disclosure of PHI.
- **Modifications to the HIPAA Privacy Rule.** Most health plans are now prohibited from using or disclosing genetic information for underwriting purposes.
- **New increased and tiered civil money penalty structure.** Fixed penalty amounts for each compliance violation are outlined.

BUSINESS ASSOCIATES NOW RESPONSIBLE FOR PHI SECURITY

Perhaps the most significant impact of the final HIPAA omnibus rule on

health care facilities is that it extends the responsibility for maintaining the security of health data to business associates and contractors. It also vastly widens the definition of *business associate* to include:

- A health information organization, e-prescribing gateway, or any other entity that provides data transmission services to a covered entity and routinely requires access to PHI
- An entity that offers a personal health record on behalf of a covered entity (but not if it offers the personal health record independently)
- A subcontractor of a covered entity or of a business associate, if the subcontractor accesses PHI of the covered entity
- An individual who creates, receives, maintains, or transmits PHI on behalf of a covered entity

These final modifications also make all the aforementioned entities—now defined as business associates—directly accountable if they violate HIPAA regulations. And while business associates are directly liable, covered entities are *also* held directly responsible for any actions of their business associates. For this reason, it's important to carefully select appropriate and compliant business associates, engage them with clear and comprehensive business associate agreements, and implement plans to monitor for ongoing compliance.

SELECTING HIPAA-COMPLIANT BUSINESS ASSOCIATES

When you're determining which business associate to hire, it's important to understand the terms that consultants and associates use to describe their services.

HIPAA-compliant refers to software and data storage systems that have controls based on three categories of safeguards: administrative, physical, and technical. Each category includes shared responsibilities for the cloud provider, along with safeguards that are the sole responsibilities of each. A "HIPAA-compliant" service has been found in compliance with the HIPAA Security and Privacy Rules.

HIPAA-certified is a term consultants sometimes use to claim their work is HIPAA-compliant, but the HHS and its Office for Civil Rights (OCR) do not certify any persons or products as "HIPAA-certified."

Providers should engage business associates that undergo annual HIPAA audits, train their staff in security, and have strict security policies and procedures in place to ensure ongoing compliance. Consider using providers that have undergone third-party audits. And finally, partner with cloud service providers that agree to sign a comprehensive business associate agreement.

USING HIPAA-COMPLIANT BUSINESS ASSOCIATE AGREEMENTS

All covered entities that engage business associates to work on their behalf must have contracts or other arrangements in place with their business associates to ensure that the business associates appropriately safeguard protected health information and use and disclose the information only as permitted or required by the Privacy Rule. Under the final HIPAA omnibus rule, these business associate agreements must include the following mandates for business associates:

- Must comply with the Security Rule with regard to electronic PHI
- Must report breaches of unsecured PHI to covered entities
- Must require that any subcontractors agree to the same restrictions and conditions that apply to the business associate
- Must comply with the same requirements of the Privacy Rule that apply to the covered entity

PENALTIES FOR NONCOMPLIANCE

The final rule incorporates the increased and tiered civil money penalty structure originally provided by the Health Information Technology for Economic and Clinical Health Act. The amount of the penalty increases with the level of culpability, capping maximum penalties for violating the same HIPAA provision at $1.5 million per year. Failure to comply with the HIPAA rules subjects providers to civil penalties of $100 to $25,000 per violation for identical violations during one calendar year.

The tiered structure for imposition of penalties identifies levels of culpability in four categories:

- **Unknowing.** The covered entity or business associate did not know, and reasonably should not have known, of the violation.
- **Reasonable cause.** The covered entity or business associate knew, or by exercising

reasonable diligence would have known, that the act or omission was a violation—but the covered entity or business associate didn't act with willful neglect.

- **Willful neglect, corrected.** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA. However, the covered entity or business associate corrected the violation within 30 days of discovery.
- **Willful neglect, uncorrected.** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the covered entity or business associate did not correct the violation within 30 days of discovery.

HIPAA COMPLIANCE AUDITS

OCR is responsible for auditing to assess controls and processes covered entities have implemented to comply with HIPAA. In 2011 OCR established a pilot audit program, and in 2013 the pilot program transitioned to a regular and comprehensive enforcement mechanism. Organizations should be prepared for a 169-item performance audit that concentrates on adherence to three rules:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Breach Notification Rule

Given the provisions of the final HIPAA omnibus rule, the audits will now include business associates in addition to covered entities.

WE'RE HERE TO HELP

Health Care facilities must update their business associate agreements and notices of privacy practices. Understanding the impacts of the final HIPAA omnibus rule is critical to maintaining the security of PHI and protecting your organization from penalties.

To learn more about maintaining HIPAA compliance and preparing your organization for an OCR HIPAA audit, contact your Moss Adams health care professional.

Chris Kradjan has consulted in the information technology field since 1996. He developed and maintains oversight of the firm's technology review compliance practices, and he provides related IT and management services to health care clients including hospitals, skilled nursing and residential extended care facilities, and others. You can reach him at (206) 302-6511 or chris.kradjan@mossadams.com.

Kevin Villanueva has been in the information technology field since 1997. He focuses on information security, disaster recovery planning, and strategic technology planning and has experience conducting technology security assessments, penetration testing, systems auditing and assessments, and other technology-related services. You can reach him at (206) 302-6542 or kevin.villanueva@mossadams.com.

TAKE THIS ARTICLE TO GO

Articles, videos, and other Moss Adams resources are also available on your mobile device.

Get the free app for iOS and Android.

- See more at: http://www.mossadams.com/articles/2014/may/new-hipaa-compliance-requirements#sthash.nhUzeBQs.dpuf

Reprinted with permission from the Washington Healthcare News. To learn more about the Washington Healthcare News visit wahcnews.com.