insights

SHUMAKER
Shumaker, Loop & Kendrick, LLP

A Newsletter from Shumaker, Loop & Kendrick, LLP | Spring 2013

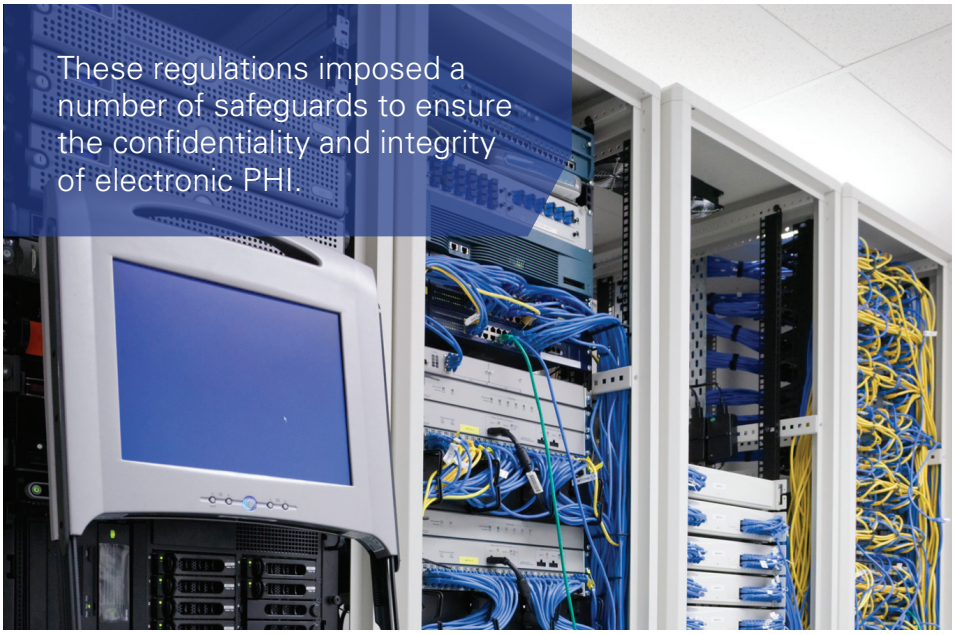
HIPAA

Not Just for Health Care Providers Anymore

The U.S. Department of Health and Human Services ("HHS") recently issued its long awaited updates to the Health Insurance Portability and Accountability Act ("HIPAA"). The HIPAA Omnibus Rule, which took effect March 23, 2013, significantly expands the reach of HIPAA outside the health care industry and ups the stakes for noncompliance. The article will address the main components of the Omnibus Rule and how they apply outside the health care industry.

By Jenifer A. Belt

The original HIPAA privacy rules were issued in 1999 and were effective April 14, 2003. The privacy regulations addressed protected health information ("PHI"), that is, individually identifiable health information that related to an individual's past, present, and future medical care and treatment or payment for that care and treatment. The privacy regulations established new limits on use and disclosure of information, and created new individual rights regarding PHI. The security regulations soon followed in 2004, and governed electronic PHI.



These regulations imposed a number of safeguards to ensure the confidentiality and integrity of electronic PHI.

Health care providers and plans alike scrambled to develop policies and procedures to comply with the original rules, with varying degrees of success; however, "much has changed in health care since HIPAA was enacted over fifteen years ago," according to HHS' press release announcing the Omnibus Rule. "The new rule will help protect patient privacy and safeguard patients' health information in an ever expanding digital age," the press release proclaims.

What's New?

The most far-reaching aspect of the Omnibus Rule is its expansion to directly regulate business associates. "Business associates" under HIPAA are defined as persons or organizations that create, receive, maintain or transmit PHI for the covered entity for purposes related to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing, or provides legal, actuarial, accounting consulting, data aggregation, management administrative,

accreditation, or financial services to or for the covered entity, if such service involves use or disclosure of PHI. The definition specifically includes health information organizations, e-prescribing gateways, or other persons who provide data transmission services, persons who offer personal health records to individuals, and subcontractors who receive PHI of business associates. 42 C.F.R. 160.103.

Under the prior rule, HHS determined it did not have authority to directly regulate business associates, so it created a business associate agreement requirement pursuant to which the covered entity was obligated to enter into a business associate agreement (BAA) that imposed all of the legal requirements applicable to the covered entity on the business associate (by contract, however, and not by law). According to the HHS Office of Civil Rights ("OCR") (the agency responsible for enforcing compliance with HIPAA), some of the most significant breaches of HIPAA have involved business associates. By determining that it had the authority to directly regulate business associates, HHS has expanded compliance obligations and potential exposure for fines and penalties to business associates. (Note, however, that even though business associates are now directly regulated, business associate agreements are still necessary.)

As the definition of business associates suggests, it extends well beyond the health care industry to a range of other industries, including records storage, data analytics, software vendors, legal and accounting firms, and many others who may come into contact with PHI in the performance of services for a third party. In addition, HHS has increased the fines and penalties that can be assessed for non-compliance with the regulations, to a maximum of $1.5 million per violation. While business associates were previously required to commit by contract to abide with the regulations, their obligation now is to comply with the law, so the stakes are higher.

What are Business Associates' Compliance Responsibilities?

Business associates have similar obligations to covered entities in ensuring the privacy and security of PHI they create, receive, maintain, or transmit. Under the Omnibus Rules, business associates are required to comply with all aspects of the security rules if they create, receive, transmit or maintain electronic PHI. Thus, for example, a law firm that receives medical records via email from a hospital in connection with a medical malpractice case must develop physical, administrative, and technical safeguards to prevent, detect, contain and correct any security violations. This would include, among others:

1. Administrative Safeguards

a. Create a security management process, to include: a required risk assessment to determine risks and vulnerabilities to electronic PHI, security measures to reduce identified risks and vulnerabilities, a sanction policy for workforce members who fail to comply with security policies and procedures, and a process to regularly review system activity.

b. Identify a security official responsible for implementing required policies and procedures.

c. Create workforce security procedures, such as procedures for electronic PHI access within the organization, workforce clearance procedures to determine access to electronic PHI is appropriate, and termination procedures to eliminate access when appropriate.

d. Create information access management policies and procedures, to include access authorization and access establishment and modification as required.

e. Implement security awareness and training, including security reminders, protection from malicious software, log-in monitoring, and password management

f. Create Security Incident Procedures.

g. Establish a Contingency Plan in the event of damage to systems containing electronic PHI, to include: a data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, and applications and data criticality analysis.

h. Perform periodic evaluations to determine ongoing compliance.

i. Enter into agreements with any third parties with which the business associate shares electronic PHI (copying firm, for example).

2. Physical Safeguards

a. Establish facility access controls to limit access to electronic PHI, including contingency operations, facility security plan, access control and validation procedures, and maintenance records.

b. Establish policies and procedures regarding workstation use for workstations that can access electronic PHI.

c. Establish workstation security for all workstations that can access electronic PHI.

d. Implement policies and procedures for device and media control to include disposal and re-use of electronic PHI, accountability, and backup and storage.

3. Technical Safeguards

a. Implement various technical controls (access control, emergency access procedures, audit controls, authentication, encryption).

4. Develop and maintain policies and procedures to ensure and demonstrate compliance.

While some of the requirements are "addressable" under the regulations (i.e. the business associate's level of implementation can be based on its risk assessment), others are required, meaning every business associate must implement the standard without exception. In addition, in the event any business associate contracts with a third party (copying firm, records storage facility, etc.) for services that involve the electronic PHI, the business associate is required to enter into an agreement with the third party to ensure the third party complies with these requirements. Moreover, the above rules only address security obligation compliance; business associates must also comply with the requirements of their business associate agreements which address their ability to use and disclose PHI (electronic and otherwise).

Risks of Non-Compliance

Now that business associates are directly covered by HIPAA, they are subject to enforcement activity. Any individual has the right to register a complaint regarding non-compliance. Since the inception of the regulations, the number of complaints for violations of the privacy rules has steadily increased each year.

In addition, Congress adopted a law in 2009 requiring reporting of security breaches. The Omnibus rule implements these statutes, requiring covered entities and business associates alike to report breaches of unsecured protected health information – covered entities must report to the affected individuals and to the government, and business associates must report to the covered entity (to report to the affected individuals and the government). A "breach" is an unauthorized access, use or disclosure of PHI in a manner not permitted by the rules. For example, if an employee who is uninvolved in the litigation the law firm is handling were to access the medical records of the plaintiff because she is an interested family member, such action would be presumed to be a breach unless a risk assessment revealed a low probability of compromise, based on the nature and extent of information involved, the unauthorized person who accessed the information, whether the PHI was actually viewed, and the extent to which risk has been mitigated.

In 2010, reported breaches affected over 5 million people, according to OCR's Annual Report to Congress on Breaches of Unsecured Protected Health Information. Because of this, the Omnibus Rule adds some "teeth" to HIPAA enforcement, and includes fines and penalties ranging from $100 to $50,000 per violation, and up to $1.5 million for repeated violations within the same year. HHS will apply a number of factors in determining the appropriate penalty, including the nature and extent of the violation (number of individuals affected and the time period during which the violation occurred) and the nature and extent of harm resulting from the violation (whether the violation caused physical, financial, or reputational harm, whether the violation hindered an individual's ability to obtain health care, history of prior compliance, and the financial condition of the business associate). Prior to the Omnibus Rule, business associates were not directly subject to these fines and penalties.

In Other News

The Omnibus Rule also makes various changes to the rules directly pertaining to health care providers and other covered entities and creates new individual rights regarding certain PHI. These changes include limitations on covered entity's use of PHI for marketing without an authorization; greater use of PHI for fundraising, and greater right of the individual to limit disclosure to a health plan in certain instances.

Deadline

The Omnibus Rule makes a number of changes to healthcare providers' ability to use and disclose information with or without a patient's authorization. In particular, the Rule gives healthcare providers some additional flexibility in terms of the kind of information they can gather and use to target fundraising efforts. Individuals must be given the opportunity to opt out of further receipt of such communications, however. The Rule also provides greater ability for healthcare providers to engage in certain activities previously considered to be marketing (and thus requiring authorization) by carving out specific activities from the definition of marketing (refill reminders, care coordination or case management so long as no remuneration is involved).

The Omnibus Rule also incorporates certain aspects of the Genetic Information Nondiscrimination Act (GINA), prohibiting health plans from using genetic information about an individual or family member for underwriting purposes.

All entities subject to the rule must comply with its requirements by September 23, 2013. HHS has developed a model business associate agreement for use by covered entities and their business associates. Covered entities and business associates alike must review and update their existing practices and procedures to ensure compliance and enter into new compliant business associate agreements (in most cases) on or before September 23, 2013.