MARSH

FEBRUARY 2013

HIPAA RULE BRINGS CHANGES TO BREACH NOTIFICATION

LEADERSHIP, KNOWLEDGE, SOLUTIONS...WORLDWIDE.

MARSH & McLENNAN COMPANIES

Faced with "sweeping changes" to the federal rules aimed at protecting patients' personal health information, health care organizations should review and, where necessary, revise their data breach notification policies. The new rules in the Health Insurance Portability and Accountability Act (HIPAA) include changes to the definition of "breach," regulatory enforcement provisions, requirements for notices of privacy practices, and the sale of protected health information (PHI).

HIPAA EVOLUTION

Health care providers, health plans, and their business associates have a strong tradition of safeguarding private health information. However, higher security standards are needed to keep pace with changing technology and the increased exchange of protected health information between covered and non-covered entities. As such, the HIPAA omnibus final rule provides clear standards for the protection of electronic protected health information (e-PHI).

Enacted in 1996, HIPAA called for the establishment of standards and requirements for transmitting certain health information and e-PHI to improve the efficiency and effectiveness of the health care system while protecting patient privacy. The standards mandated in the Act protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. The rule was modified several times, although the 2009 interim rule remained in effect until January 2013. The 2009 rule issued regulations requiring health care providers, health plans, and other entities covered by HIPAA to notify individuals when their health information is breached. These breach notification regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Regulations developed by the Office of Civil Rights (OCR) require health care providers and other HIPAA-covered entities to promptly notify affected individuals of a breach, and to notify the Health and Human Services (HHS) secretary and the media when a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals were to be reported to the HHS secretary annually.

The rule also defined "business associates" of covered entities and their requirements regarding data breach notification. Under HIPAA section 160.103, business associates are generally defined as a person or organization — other than a member of a covered entity's workforce — that performs certain functions or activities on behalf of, or provides services to, a covered entity that involve the use or disclosure of individually identifiable health information. The activities include such things as claims processing, data analysis, utilization review, and billing. The law's purpose was to ensure that covered entities and business associates are accountable to HHS and to individuals for proper safeguarding of the private information entrusted within their care. The regulations clarify however, that entities securing health information through encryption or destruction are relieved from having to notify in the event of a breach of such information.

NEW DEFINITIONS AND STANDARDS

Those rules remained in effect until the OCR adopted the final rule on January 29, 2013. OCR Director Leon Rodriguez said at that time: "This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented." Most notably, the rule modified the definition of breach from the 2009 omnibus rule, which had defined "breach" as the "acquisition, access, use or disclosure of protected health information in a manner not permitted under [the privacy rule] which compromises the security or privacy of the protected health information." Further, the phrase "compromises the security or privacy of PHI" was defined as "posing a significant risk of financial, reputational, or other harm to the individual."

Under the final rule, breach is defined as "an acquisition, access, use, or disclosure of protected health information in a manner not permitted…[and] *is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised* [emphasis added]." According to HHS, "breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that PHI has been compromised."

To demonstrate that there is a low probability that a breach compromised PHI, a covered entity or business associate must perform a risk assessment that addresses the following minimum standards:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made, whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.

In addition to a tougher breach reporting standard, the omnibus rule expands HHS' enforcement over business associates by requiring them to execute agreements to comply with the requirements imposed on them by HIPAA. The rule also extends this requirement to subcontractors that receive or transmit PHI on their behalf and sets forth new requirements for notices of privacy practices for all covered entities. Although the sale of PHI without authorization is prohibited, as is the use of PHI for marketing or research purposes, the rule provides certain exceptions. Most notably, an authorization to sell PHI must state that the disclosure will result in remuneration to the covered entity.

RISK MANAGEMENT STEPS

Given the changes to existing HIPAA regulations, health care organizations and covered entities are faced with a myriad of obstacles and significant work in order to avoid penalties for noncompliance. It is recommended that, at a minimum, they review and revise policies and procedures concerning breach notification and the sale of PHI, and develop new forms for business associates to ensure they extend to subcontractors.

Risk managers at affected entities also should review policies regarding PHI use for fundraising, requests to transmit PHI to third persons, disclosure of immunization records, and authorizations for the use and sale of PHI and disclosure of PHI for paid marketing. In addition, business associates and any entity that transmits PHI should, if they have not already done so, perform risk assessments and carefully review their relationships with subcontractors. The entities may also want to seek clarification of language that clearly defines the roles and responsibilities of each party.

As evidenced by recent resolutions with the OCR, no data breach is too small to warrant attention, and recent fines for noncompliance and resolutions agreements are broad, ranging from $50,000 to $2.25 million. The final rule goes into effect on March 26, 2013, but business associates and covered entities will have 180 days beyond the effective date — until September 23, 2013 — to come into compliance.

CONCLUSION: BE DILIGENT

Several key factors must be considered to determine whether PHI has been compromised, including:

- The nature and extent of the violation.
- The nature and extent of resulting harm.
- Whether the violation hindered the ability to obtain health care.
- The extent to which the risk has been mitigated.

Since the final rule places the burden on the covered entity to demonstrate that there is a low probability that PHI has been compromised before the impermissible use or disclosure of PHI is presumed to be a breach, health care providers and covered entities must remain diligent in notification to affected individuals of *any* inappropriate uses or disclosure of PHI.

Data Breaches By The Numbers

Health care organizations are among those most at risk from data breaches. Consider the following:

- 94% of health care organizations suffered a data breach in the past two years; 45% suffered more than five such incidents (compared with 29% in 2010).[1]
- Health care organizations accounted for the largest percentage of data breaches identified in both the third and fourth quarters of 2011 (39% and 40%, respectively).[2]
- The average economic impact of a data breach in 2011 and 2012 for health care organizations participating in the study was $2.4 million, up from $400,000 in 2010. In the aggregate, the cost to the health care industry is staggering — as high as $7 billion annually.
- The average number of lost or stolen records per breach was 2,769.
- 91% of hospitals surveyed use cloud-based services; however, 47% do not have confidence in the cloud's security and only 23% are somewhat confident.[3]

---

1 "Third Annual Benchmark Study on Patient Privacy and Data Security" sponsored by ID Experts, Corp., December 2012

2 Navigant Information Security & Data Breach Report, April 2012 Update.

3 "Third Annual Benchmark Study on Patient Privacy and Data Security" sponsored by ID Experts, Corp., December 2012

MARSH

For further information, please contact your local Marsh office or visit our website at marsh.com

ROBERT PARISI
FINPRO Network and Security Practice Leader
robert.parisi@marsh.com
+1 212 345 5924

ELISSA DOROFF
elissa.k.doroff@marsh.com
+1 212 345 6404

RICHARD DePIERO
richard.depiero@marsh.com
+1 212 345 1761

JOHN O'DONNELL
john.odonnell@marsh.com
+1 212 345 0038

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh's prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.

Copyright 2013 Marsh Inc. All rights reserved. Compliance MA13-12147 4783