HEALTH LAW

Data Breaches In Health Care

Heightened risks bring on emerging insurance and legal considerations

By MARIA PEPE VanDerLAAN, MELISSA A. FEDERICO and STEPHANIE SOBKOWIAK

Technology within the health-care industry is changing rapidly. With the expansion of electronic information comes the risk of loss. This risk is heightened in the health-care industry because recent regulatory changes have expanded the responsibility of health-care organizations and their business associates to protect health information. Unfortunately, traditional insurance policies do not always provide the necessary coverage, and health-care organizations and their business associates should consider purchasing cyberrisk or specialty policies to protect themselves.

The Risk

Health care is now ranked among the highest industries to be affected by or at risk of data breaches, comprising more than 36 percent of all data breaches (Symantec Corp., Internet Security Threat Report 2013). The average cost per record of a health-care data breach in 2011 was $240, which is 24 percent higher than the cost per record of the average data breach (Ponemon Institute, 2011 Cost of Data Breach Study United States, March 2012).

According to a February 2014 report by the SANS Institute, current health-care security practices and strategies "are not keeping pace with attack volumes" and attackers are bypassing perimeter protections en masse without the need to use stealth techniques. In 2014 alone, hospitals in Connecticut, Vermont, Delaware, Virginia, Colorado and Texas have confirmed security breaches affecting thousands of patients' personal and protected health information (PHI). Just in the last few days, we received word that two prominent New York organizations paid $4.8 million to settle charges that they potentially violated HIPAA due to a physician's inadvertent release of PHI on the internet.

HITECH And The Omnibus Rule

The Health Insurance Portability and Accounting Act and its implementing regulations are the main drivers for health-care organizations' data privacy and security compliance programs and related cyber and breach response coverage needs. In 2009, HIPAA was amended pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH) to require covered entities to notify individuals whose unsecured PHI has been or is reasonably believed to have been accessed because of a breach. Effective Sept. 23, 2013, any impermissible disclosure of PHI is now presumed to be a breach that triggers notification, unless it can be demonstrated that there is a low probability that the PHI has been compromised. This change was part of a set of regulations referred to as the Omnibus Rule.

The Omnibus Rule also implemented a significant change for business associates of HIPAA-covered entities by making them directly liable for HIPAA violations. This means that scores of health-care service providers (such as billing organizations, banks providing health-care lock box services, cloud providers, law firms with health-care clients, and third-party administrators to health plans) should be establishing HIPAA-compliance programs and examining the need for risk transfer instruments.

Previously under HIPAA, business associates were obligated contractually under the terms of business associate agreements to provide HIPAA protections regarding PHI used in the performance of services on behalf of covered entities. HITECH mandated that business associates be directly regulated under HIPAA and the Omnibus Rule set those requirements in motion. The Omnibus Rule also broadened the definition of business associate, notably to include subcontractors of business associates. This means that, like business associates, subcontractors to business associates are subject to direct liability and enforcement activity for HIPAA compliance failures.

Traditional Coverage

Three of the chief risks to the health-care industry due to these recent regulatory changes are investigation costs, fines and penalties, and notification costs. The pre-2001 commercial general liability (CGL) forms drafted by the Insurance Services Office (ISO) allowed for relatively broad arguments for coverage, defining "property damage" as "physical injury to tangible property." Since 2001, the ISO has added endorsements and amended this definition to specifically exclude these risks and restrict coverage. The ISO recently filed a number of data breach exclusionary endorsements for use with its standard-form primary, excess and umbrella CGL policies effective May 2014, which appear intended to exclude coverage for hacking claims.

That being said, some courts have held that traditional policies cover business associates for HIPAA violations. Last year, a California court in *Cottage Health System v. Travelers Casualty & Insurance* held that doctors (who were business associates of the hospital) were covered as "independent contractors" under a directors and officers insurance policy. The court determined that the definition of independent contractor (defined as being under the "exclusive direction" of the hospital) was ambiguous and, therefore, construed the term in favor of the policyholder.

In February, a California district court held that health-care data loss was covered as a "personal and advertising injury" under a CGL policy in *Hartford Casualty Insurance v. Corcino & Associates*. The insurer argued that the underlying plaintiffs' requested statutory relief barred coverage under the exclusion for injury "[a]rising out of the violation of a person's right to privacy created by any state or federal act." The district court concluded that the exclusion did not apply because the applicable California statutes were intended to codify existing rights, and not create new privacy rights. Accordingly, the loss was covered.

Some insurers have addressed health-care risks in traditional policies by expanding the definition of "loss" to include HIPAA penalties. To address the significant increase in notification costs under the new Omnibus Rule, certain insurers are offering an information privacy coverage endorsement that they present as specifically tailored to cover HIPAA fines and penalties and notification costs. One way investigative costs have been addressed is through the inclusion of a privacy coverage endorsement that covers "all claims" related to "any HIPAA proceeding." In defining "HIPAA proceeding," the language might state:

"HIPAA proceeding" means an administrative proceeding, including a complaint, investigation or hearing instituted against you by the Department of Health and Human Services or its designee alleging a violation of responsibilities or duties imposed on you under ... HIPAA ... with respect to the management of confidential health information.

This broad definition can be constructed to capture even more risk by including defense costs in proceedings brought by state attorneys general under HITECH.

Cyberliability Coverage

Cyberrisk policies were first introduced in the mid-1990s and provide third-party liability and first-party coverages for losses in addition to those due to HIPAA violations. For example, one policy promises reimbursement for "Security Breach Notification Expenses," which includes expenses to communicate with the persons whose information was accessed without their authorization; maintain a call center; provide up to 365 days of credit-monitoring services; and any other expenses necessary to comply with any applicable security breach notification law.

When a breach happens, even if caused by a business associate, HIPAA-covered entities typically are the ones who incur the costs. Since the Omnibus Rule took effect, more and more HIPAA-covered entities have required their business associates to purchase cyberliability coverage to indemnify them in the event of a data breach and/or security incident.

Conclusion

Judicial construction of these emerging policies is underdeveloped at this time. Even in this uncertain environment, health-care organizations and their business associates must attempt to secure sufficient coverage for these risks. The failure to do so could result in an unwelcome, and very expensive, cost that will detrimentally impact their bottom line. ■


Maria Pepe VanDerLaan


Melissa A. Federico


Stephanie Sobkowiak

Maria Pepe VanDerLaan and Melissa A. Federico are members of Murtha Cullina's litigation department and insurance recovery practice group. Stephanie Sobkowiak is a member of Murtha Cullina's health-care practice group.