Insurance Coverage for Health Care Cyber Risks

Arden B. Levy
Miller Friel PLLC
Washington, DC

Introduction

Data privacy and cybersecurity issues have skyrocketed in importance for health care organizations over the past few years. In that time, providers and vendors have widely adopted electronic health record (EHR) systems, with new requirements to establish and upgrade data systems to comply with privacy rules and regulations and enforcement mechanisms, in particular those implemented and overseen by the Health Insurance Portability and Accountability Act (HIPAA), as amended, and under the Health Information Technology for Economic and Clinical Health (HITECH) Act. This changing data landscape has meant that providers now have far greater responsibility for maintaining compliance protocols and safeguarding the privacy and security of protected health information (PHI)—such as patient records. At the same time, the growing likelihood of a cyberattack or data breach of those records has grown exponentially, greatly expanding the potential liability for organizations.

The resulting costs associated with a cyberattack or data breach could be enormous, and therefore insurance to pay for those costs should be a top consideration. For example, as reflected in The Ponemon Institute’s “2014 Cost of Data Breach Study: Global Analysis,” the average total cost of a data breach for the companies participating in [its] research [had] increased 15 percent to $3.5 million.” The study reported the average cost to a health care organization per record of a health care data breach is $459.4 Those costs arise on multiple fronts, including but not limited to: repairing damaged or compromised software and hardware systems; reconstructing data;5 the legal and forensics costs associated with investigating and reporting a data breach notification; reimbursing customers whose PHI was impacted and rebuilding relationships;6 responding to government inquiries (including the risk of criminal or civil fines or penalties being assessed for HIPAA violations);7 and defending against third-party lawsuits. A priority for any policyholder is to secure as much insurance coverage as possible to cover these costs.

Health care organizations and providers should begin with the assumption that there is coverage, even if insurers or brokers state otherwise. For example, the Omnibus Rule’s provision for different degrees of culpability and penalty levels under HIPAA means that coverage for fines and penalties may not be excluded, even if it is sought for willful statutory damages.8 Similarly, different levels of culpability under HIPAA mean that fraud exclusions may not apply. Coverage should be assumed, and not the inverse. To best position themselves for coverage, policyholders should evaluate their entire insurance program, ranging from cyber or HIPAA coverage, to traditional commercial or Directors & Officers (D&O) policies, and pursue a strategy for coverage under those policies. The below considerations highlight some of the complex issues that providers and vendors typically must consider in order to secure insurance coverage that will pay for defense and indemnity costs arising out of cyber issues.

Evaluate and Consider All the Company’s Insurance Policies for Coverage of Both Defense and Indemnity Costs

Cyber Policies may Provide Certain Coverage

Cyber coverage is an evolving legal landscape. On the one hand, insurance carriers have developed a slew of new cyber insurance products, and have enlisted insurance brokers to sell those policies in response to the ever-increasing demand. These cyber-specific policies can provide excellent coverage. On the other hand, however, these policies often require considerable rewrites to achieve the desired result. Perhaps an even bigger problem is that insurers are denying coverage under cyber-specific policies as well.

Reliance on cyber coverage demands attention to certain provisions in particular. A recent California case, which was dismissed on other grounds, provides a cautionary tale for reliance on cyber coverage. In Columbia Cas. Co. v. Cottage
The fact that CGL policies sometimes include specific cyber exclusions is a strong indicator that current standard-form business insurance should not be overlooked and may provide coverage. The arguments for coverage of losses arising from a third-party claim or investigation under CGL coverage are simple and straightforward. Most General Liability policies contain a separate grant of coverage for “Personal and Advertising Injury.” This grant affords coverage for any “oral and written publication, in any manner, that violates a person’s right to privacy.”9 Accordingly, if someone took private information, and released that to others, coverage should be provided.

CGL Policies Provide Coverage for Losses Arising from a Third-Party Claim

A cyber policy should be tailored to a health care provider’s risks and should contain a sufficiently broad definition of “loss” in order to obligate the insurer to pay for damages paid in connection with a failure to comply with HIPAA (or analogous state) requirements. Also, a cyber policy should be tailored to a provider’s usage of third-party vendors and of the “cloud,” so that it covers the acts and omissions by third parties, or data in the custody of third parties.

Courts addressing coverage under CGL insurance policies for cyber liability have often found coverage.10 Sometimes a court makes that determination based on whether the information actually was, or could have been, accessed.11

Two courts recently have found “publication” where patient information was posted on the internet and publicly available. In Hartford Casualty Insurance Co. v. Corcino & Associates, 2013 WL 5687527 (C.D. Cal. Oct. 7, 2013), the court found coverage for a hospital’s loss arising out of two class actions alleging disclosure of patients’ confidential medical records by “publication”—posting on a public website. Likewise, in Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC, 35 F. Supp. 3d 765, 770-71 (E.D. Va. 2014), a health care provider allegedly “failed to safeguard the confidential medical records of patients” where its third-party vendor responsible for the electronic storage and maintenance of those records made some patient records publicly accessible and available on the internet without any security restriction. By posting the information on the internet, there was a potential publication, triggering coverage for an underlying class action.

CGL Policies Provide Coverage for an Insured’s Direct Losses

First-party commercial property coverage provides coverage for losses related to property damage and business interruption losses that result from a cyberattack or data theft.

For example, in Lambrecht & Associates v. State Farm Lloyds, 119 S.W.3d 16 (Tex. App. 2003), the court found coverage for the replacement costs for the insured’s server, operating system, and data damaged by a hacker’s computer virus attack. Similarly, in Southeast Mental Health Center v. Pacific Insurance Co., 439 F. Supp. 2d 831 (W.D. Tenn. 2006), where a clinic lost electronic and telephone service as a result of storm damage, resulting in damage to the clinic’s pharmacy computer and lost data, and plaintiff was forced to suspend operations, the court found coverage for the resulting loss of business income.

Other Policies may Provide Coverage

A provider or hospital system may have other insurance coverage contained within its insurance program that is tailored to cover losses specific to HIPAA compliance or violations or cyberattacks. For example, a policy provision that excludes coverage for losses arising from fines or penalties may specifically allow for coverage of “HIPAA penalties.” A policy also may provide for coverage of the costs to notify patients, for forensic or investigation costs for a “HIPAA proceeding” or proceedings brought by a state attorney general under the HITECH Act, or other regulatory proceeding.

It is further possible that a policy may provide coverage for a third-party act or omission made by a vendor, or “business associate,” who is maintaining or storing the data. Such a provision addresses the expanded liability imposed by recent amendments to HIPAA that would hold a provider liable for the violations of its outside vendor even if not aware of any pattern and practice of violations.12

Finally, it is possible that there also may be coverage for data losses under other insurance policies, such as D&O, Errors & Omissions, property, or crime policies. An example is a HIPAA subpoena that is simply part of an investigation brought pursuant to authorization under HIPAA, but not specifically related to violations for failing to comply with data security obligations in HIPAA. In that instance, a policyholder may secure coverage under its D&O policy providing for coverage of government investigations.
Pursue Coverage for Statutory Damages

Policyholders seeking coverage are often told by their insurance carriers that their insurance policy does not cover statutory damages. However, policyholders should not accept insurance company coverage denials that are based on an improper labeling of damages. Rather, policyholders should conduct a thorough analysis of policy language and damages alleged, and fight for all of the coverage to which they are entitled.

Damages may be Compensatory or Otherwise Covered

In order to avoid coverage, insurers may label damages as “restitution,” or treat them as “punitive” in nature. They also may argue that such damages constitute an allegedly uncovered “fine or penalty.” Yet, as recently illustrated, when insurance carriers are challenged on these denials, they are often proven wrong by the courts.13

The Navigators court held the errors and omissions insurance policy even covered statutory damages for willful violations, even though the policy excluded coverage for fines and penalties. In Navigators, it was alleged that the policyholder Sterling willfully violated the Fair Credit Reporting Act (FCRA) by providing false information to employers, who relied on that information to terminate the plaintiffs’ employment. Sterling sought coverage under its policy, which covered all sums that the insured became legally obligated to pay as damages, but excluded fines and penalties. The insurer, Navigators, denied coverage and contended that the damages sought under FCRA were excluded penalties. Sterling disagreed and contended that the damages sought were not penalties, but were compensatory in nature.

Notably, the court reasoned that resolution of the coverage dispute depended on the interpretation of FCRA. Under FCRA, a plaintiff can seek either its actual damages or statutory damages between $100 and $1000 per violation, as well as punitive damages. The court noted that the underlying plaintiffs sought only statutory damages for willful violations. The court stated that, depending on the statute, such statutory damages can be compensatory, punitive, or both. Under FCRA, the court found for three reasons “that the statutory damages function primarily as compensation.”

First, because “actual damages are compensatory, statutory damages that substitute only for those actual damages are also compensatory.” Second, statutory damages under FCRA are designed to provide a remedy when actual damages are difficult to calculate. Finally, the court noted that the statute provided a separate remedy for punitive damages, so the other damages sought are more logically considered to be compensatory. The policy provided coverage because damages were compensatory in nature. Hence, they were not subject to the fines or penalties exclusion as Navigators contended.

Similarly, what also matters is determining whether the damages are remedial or compensatory in nature. Courts determining coverage under traditional policies while evaluating how to classify monetary payments due under statutes have looked to the intent behind the remedy and whether the payment is remedial or compensatory in nature. For example, in Universal Underwriters Insurance Co. v. Lou Fusz Auto Network, Inc., 401 F.3d 876 (8th Cir. 2005), the court addressed whether required payments under the Telephone Consumer Protection Act (TCPA) for damages for each separate violation constituted damages where the garage liability policy at issue specifically excluded coverage for fines and penalties. Because the TCPA was meant to be both punitive and remedial, and the payments contained some remedial nature, they were not “penalties,” and the court found there was coverage.16 Similarly, in Visa Inc. v. Certain Underwriters at Lloyds, London, 2012 WL 10161619 (Cal. Super. Jan. 6, 2012), a California court held, in an order denying the insurer’s motion for judgment on the pleadings, that the statutory damages under the California Invasion of Privacy Act were not “penalties” or “sanctions.”

Structure Settlement so Damages Are Properly Characterized for Coverage

The characterization of any damages is particularly important because if they can be characterized as compensatory, they may be covered. Additionally, for HIPAA matters under the new Omnibus Rules, providers may be required to pay even if they had no knowledge of a violation.17 What this means is that settlement amounts that might previously have been excluded from coverage as fines or penalties for intentional or willful conduct might now be covered. Moreover, many states have held that it is not against public policy for an insurance carrier to pay for fines and penalties. Finally, certain portions of a settlement, such as plaintiffs’ attorneys’ fees, are traditionally considered covered by insurers. For these reasons, policyholders should keep in mind insurance coverage at all stages of underlying investigations or litigation.

Conclusion

In most cyberattack or data breach situations, there are good arguments that coverage is triggered, and that is often the case under traditional CGL policies. Courts are generally aligned in favor of coverage if data was disseminated to third parties. Experienced coverage counsel’s careful examination of insurance policies and the nature of a cyberattack or data breach may be important to preserve coverage. Failure to take this approach could result in an unwelcome and expensive set of costs.
1. HITECH is a series of statutory provisions within the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5; see ARRA Division A, Title XIII—Health Information Technology, Section 13001.


4. See id., 5 n.4, 7.

5. See HITECH Act, Section 13402(h).


7. For example, HITECH increased the amount of potential civil penalties—which start at $100 per violation and increase up to $50,000 per violation, with a yearly maximum of $1.5 million for similar violations—depending on the nature of the violation. See 78 Fed. Reg. 5583 (Jan. 25, 2013), discussing section 160.404, HITECH, Section 13410(d).


9. See ISO standard form CG 00 01 12 07, defining as “oral or written publication, in any manner, of material that violates a person’s right of privacy.”


11. See, e.g., Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 317 Conn. 46, 115 A.3d 458 (2015) (finding that where stolen tapes contained personal information that could not be read by a personal computer, no third party had accessed the information, and no person had suffered injuries from loss of the tapes).

12. See 78 Fed. Reg. 5566, 5580-81 (Jan. 25, 2013). The agreement must grant the CE “the authority to direct the performance of the service provided by its business associate after the relationship was established”.


14. Slip op. at 8.

15. Id.

16. See id.

17. See 78 Fed. Reg. 5566, 5586 (Table 2) and 5586 (Jan. 25, 2013).