Data Breaches in Health Care: New or Heightened Risks, Emerging Insurance and Legal Considerations

Arden B. Levy
Miller Friel, PLLC
2101 L Street, NW, Suite 1000
Washington, D.C. 20037
Tel. 202.760.3158 Fax. 202.459.9537

2050 Ballenger Avenue, Suite 200
Alexandria, VA 22314
Tel. 703.519.6800 Cell 703.850.0145
Levya@millerfriel.com www.millerfriel.com

Maria Pepe VanDerLaan
Murtha Cullina, LLP
185 Asylum Street, Hartford, CT 06103 (Resident Office)
Direct 860.240.6128 Main 860.240.6000
mvanderlaan@murthalaw.com www.murthalaw.com

New Haven Office: Two Whitney Avenue, New Haven, CT Tel. 203.772.7700
Stamford Office: 177 Broad Street, Stamford, CT Tel. 203.653.5400
Boston Office: 99 High Street, Boston, MA Tel. 617.457.4000
Woburn Office: 600 Unicom Park Drive, Woburn, MA 01801 Tel. 781.933.5505

Ngozi Nnaji, MS, Vice President, Willis of Connecticut, LLC
185 Asylum Street, Hartford, CT 06103
Direct 860.756.7337
Ngozi.nnaji@willis.com www.willis.com

Katherine M. Keefe
Breach Response Services
BEAZLEY GROUP
Two Liberty Place, 50 S. 16th Street, Suite 2700
Philadelphia, PA 19102
Direct 215.446.8421 Cell 610.724.4421
Katherine.keefe@beazley.com
I. INTRODUCTION

The pace of technology changes, innovation, and business adoption in the last three to five years has profoundly altered the business landscape. It is reported that the world’s stock of data is currently doubling every 20 months and that the number of internet connected devices has reached twelve billion. Data visualization, wireless communications, and cloud infrastructure are extending the power and reach of information and communication and data capabilities.

Do developments in information and communication technologies lead to developments in risk? Of course. And this increased risk affects industries across the board, including health care. Whereas the health care industry was once viewed as existing outside the purview of advancements in information and communication technologies to a degree, that perception has now changed. That change has been rapid due to, in large part, the very recent adoption of electronic health record (EHR) systems among providers. A massive expansion of EHR is at the center of quickly evolving federal government programs and legislation regarding the use and maintenance of EHR. And, since EHR consists of electronic protected health information, privacy and security protections are necessary and required by law. Failure to adopt such protections increase potential legal liability. Regulatory changes related to health care and health information will also affect entities that maintain data systems as part of their daily business even if they do not view themselves as participating in the health care industry.

These materials and the related presentation address the statutory and regulatory landscape that relates to the protection of PHI and ePHI1 in the health care context and the various obligations that landscape imposes on health care providers, health plans or their vendors. The risks that arise from these obligations also will be addressed as will the state of insurance and insurance coverage disputes. We end with considerations for policyholders as these issues and the marketplace evolve in the near term.

---

1 HIPAA governs both “protected health information” (PHI) in any form (paper, verbal or electronic) and “electronic protected health information” (ePHI) which is a subset of PHI; this paper’s focus is primarily on risks associated with the maintenance of computer systems containing ePHI. However, the authors note that failures to secure PHI in any form raise many of these same concerns and liabilities.
II. CYBER COVERAGE CONCERNS IN HEALTH CARE: SHARPENED BY A LIVELY REGULATORY CLIMATE

For health care organizations (including hospitals, health systems, physician groups, ancillary health care providers and health plans) and their vendors, data privacy and security and the need for cyber coverage is becoming of primary importance as the result of regulatory requirements and enforcement activities on both federal and state levels. In fact, the health care sector ranked among the highest industries to be affected by or at risk of data breaches, comprising just over 36% of all data breaches.\(^2\) Further, 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 (the average data breach was $194).\(^3\) Insight into the complex regulatory requirements for health care privacy and security underscores emerging and potentially significant risks facing health care organizations.

---
\(^2\) 18 Symantec Corporation, *Internet Security Threat Report 2013*  
\(^3\) Ponemon Institute LLC, *2011 Cost of Data Breach Study United States*, 5-7 (March 2012).
A. HIPAA: HITECH and the Omnibus Rule

The Health Care Portability and Accountability Act of 1986 and its implementing regulations (“HIPAA”) is the main driver for health care organizations’ data privacy and security compliance programs and related cyber and breach response coverage needs. HIPAA established the privacy and security regulatory framework for “covered entities”, which include health care providers, health plans and clearinghouses for certain electronic health care transactions. Under HIPAA’s Privacy and Security Rules, covered entities must safeguard the confidentiality of protected health information (PHI), train workforce members on privacy and security policies and procedures and maintain written agreements with certain vendors called “business associates”, to name a few key HIPAA requirements.

HIPAA does not provide a private right of action. The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) is the federal agency that enforces HIPAA through a variety of means including a complaint and investigation process, statutorily mandated audits and statutory fines and penalties.

Since its inception, HIPAA has been amended pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH). Also, new HIPAA regulations have been implemented under the Omnibus Rule that change covered entities’ obligations with respect to the privacy and security of PHI and the obligation to notify affected individuals of breaches of PHI.

1. HITECH and its Interim Regulations: Breach Notification

HITECH amended HIPAA to require covered entities to notify individuals whose unsecured PHI has been or is reasonably believed to have been accessed, acquired or disclosed because of a breach of the PHI. HITECH also imposed a requirement on business associates to notify covered entities of breaches of unsecured PHI and required such notification to include the identity of each individual whose unsecured PHI was breached.

“Unsecured PHI” is defined by HITECH as PHI that is not secured through the use of technologies or methodologies, as specified in guidance by the Secretary of HHS, that render the PHI unusable, unreadable or indecipherable to unauthorized individuals. HHS issued guidance which defines secured PHI as PHI that is encrypted or destroyed according to standards established by the National Institute of Standards and Technology.

Under HITECH, “breach” is defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information. HITECH carved out several exceptions to what is considered a breach including situations where the PHI would not reasonably have been retained, certain good faith access or use of PHI by

---

4 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.
5 HITECH Act, Section 13402(a).
6 HITECH Act, Section 13402(h).
8 HITECH Act, Section 13400.
employees of covered entities and business associates, and certain inadvertent disclosures of PHI within covered entities and business associates.

HITECH’s key statutory breach notification obligations include requirements regarding the timing, method and content of breach notifications, and established requirements for breaches involving more than 500 persons, including immediate notification to the OCR and notification to the media. Another key statutory provision is the requirement for substitute notice by conspicuous posting in the event of insufficient or out-of-date address information for 10 or more affected individuals.

The Interim Final Rule on Breach Notification for Unsecured Protected Health Information (IFR) took effect on September 23, 2009 and implemented HITECH’s breach notification requirements. While the IFR largely implemented all of HITECH’s breach notification requirements, it clarified or expanded statutory provisions in certain areas.

The IFR adopted HITECH’s definition of “breach” (the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or the privacy of the PHI), and further defined “compromises” to mean posing “a significant risk of financial, reputational or other harm to the individual”9 (“risk of harm standard”). The IFR’s administrative provisions place the burden of proof on covered entities and business associates to demonstrate that either notifications were made or that the use and disclosure did not constitute a breach. The OCR made clear in the preamble to the IFR that fact-specific risk of harm assessments must be conducted and documented.10

Other HITECH breach notification requirements implemented under the IFR included:

- Written notification by first-class mail must be provided to affected individuals no later than 60 days after discovery of a breach;
- Notification must contain: a brief description of the breach, date of the breach, date of discovery of the breach, types of unsecured PHI involved in the breach, steps individuals should take to protect themselves, description of covered entity’s steps to investigate breach, mitigate harm and protect against further breaches, and contact information for individuals to ask questions or learn additional information;
- Substitute notice must be provided in the event that there is insufficient or out-of-date contact information for 10 or more individuals. Substitute notice can take the form of a conspicuous posting either on the covered entity’s web site for 90 days or as a notice in major print or broadcast media in the areas where the affected individuals are likely to reside;
- Notification to the media must be provided for a breach involving more than 500 residents of a state or jurisdiction;

• Notification to OCR must be made contemporaneously with individual notification for breaches involving 500 or more individuals and must be made annually not later than 60 days from the end of the calendar year for breaches involving less than 500 individuals; and
• Notification by a business associate must be made to the covered entity no later than 60 days after discovery of a breach.

2. The Omnibus Rule

a. Breach Standard Now Changed

Last year, OCR published a series of HIPAA regulations governing several aspects of HIPAA, including breach notification. This set of regulations is referred to as the Omnibus Rule.

The Omnibus Rule changed the approach to determining whether a breach has occurred. As of September 23, 2013, the compliance date of the Omnibus Rule, no longer are breaches determined using the “risk of harm” standard implemented under the IFR. Instead, any impermissible acquisition, access, use or disclosure of PHI is now presumed to be a breach that triggers breach notification, unless it can be demonstrated that there is a low probability that the PHI has been compromised. Such demonstration must be through a documented risk assessment that addresses at least the following four factors:

• The nature and the extent of the PHI involved
• Unauthorized users or recipients of the PHI
• Was the PHI actually acquired or used?
• The extent to which the risk to the PHI has been mitigated

Through the creation of a presumption of breach, the government has created a climate in which covered entities, if at all in doubt, will likely treat patient data incidents as breaches requiring notification. In fact, this is behavior that the government is seeking to promote given its comment in the prefatory language to the Omnibus Rule that the previously applicable risk of harm standard was too subjective and set too high of a bar for triggering breach notification.12

The Omnibus Rule left unchanged most of the breach notification requirements contained in the IFR. Covered entities and business associates must continue to comply with the breach notification requirements established by HITECH and the IFR discussed above.

13 45 C.F.R. Section 164, Subpart D.
b. **Business Associates (“BA”)**

The Omnibus Rule implemented a significant change for business associates of HIPAA covered entities. Now, business associates are directly liable for HIPAA violations. This means that scores of categories of health care service providers (billing organizations, banks providing health care lock box services, cloud providers, law firms with health care clients, and third party administrators to health plans, to name a few), should be establishing HIPAA compliance programs and examining the need for risk transfer instruments. Typically, this also means that business associates should be updating and revising their own privacy policies, such as limiting access to data for marketing or fundraising purposes.

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 effective September 23, 2013. Also, the Omnibus Rule 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.\(^\text{14}\)

**B. HIPAA Penalties and Enforcement Activities**

The federal government’s power to levy criminal and civil fines and penalties for HIPAA violations has been strengthened and clarified since the inception of HIPAA. HITECH as recently implemented by the Omnibus Rule effective as of March 26, 2013, 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 for similar violations—\(^\text{15}\) depending on the nature of the violation. HITECH also clarified the circumstances under which an individual, versus a HIPAA covered entity, may be prosecuted for a HIPAA crime.

HITECH empowered state attorneys general to enforce HIPAA by bringing civil actions on behalf of residents of the state as long as no federal action has been commenced with respect the same violation.\(^\text{16}\) The right of an attorney general to enforce HIPAA in this manner is in addition to any other powers the attorney general may have under state law.

To enforce HIPAA, OCR investigates HIPAA complaints and HIPAA breaches and will often require corrective measures of an offending covered entity. For more serious violations, OCR uses a negotiated process culminating in the execution of a Resolution Agreement to extract monetary payments from violating health care entities. A Resolution Agreement is an agreement under which the violating entity agrees to perform specific HIPAA compliance obligations and report to OCR, for a period of three years during which OCR monitors the entity’s performance. The entity also agrees to make a Resolution Agreement.

---


Payment when entering into the Resolution Agreement. If the entity does not satisfy the terms of the Resolution Agreement, civil monetary penalties may be additionally applied.

A summary list of 2013 Resolution Payments is below:\(^\text{17}\):

- $1.2 million payment by health plan: PHI of 344,579 health plan enrollees left on leased photocopier
- $1.7 million payment by health plan: PHI of 612,402 health plan enrollees accessible on internet
- $275,000 payment by medical center: Media disclosure by medical center executives about medical services provided to a patient
- $400,000 payment by university outpatient clinic: PHI of 17,500 patients were left unsecured due to disabling of firewalls
- $150,000 payment by physician practice: PHI of 2,200 patients on unencrypted thumb drive stolen from staff member’s car

OCR’s active enforcement initiatives, exemplified by these Resolution Payments, clearly indicate far more attention to health information privacy and security by the federal government. Thus, typical business activity engaged in by a health care organization, such as an acquisition of a hospital or health system, or merging physician practices, can create risks if the right data security compliance systems are not put into place immediately.\(^\text{18}\)

C. State Law Data Breach Notification Requirements

In addition to HIPAA, health care organizations and their vendors also must be mindful of state data breach notification laws. To date, 46 states and the District of Columbia have some form of data breach notification laws. State data breach notification laws each differ in terms of how PHI is defined, what triggers a data breach response, whether state regulatory agencies must be notified, and the timing and content of notifications to affected residents.

State data breach notification laws present challenges for health care organizations from a couple of perspectives. Obviously, organizations that operate in multiple states must adhere to the laws of the states in which they operate. In addition, state data breach laws apply to the PHI of the residents of the state. Consequently, health care organizations must identify the state of residence of their patients/enrollees in order to comply with all relevant laws in a given data breach.

\(^{17}\) For complete details of all OCR Resolution Agreements, see http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

\(^{18}\) For example, a new gray area may occur where a glitch occurs in the system, or malicious code destroys or alters patient data on the electronic system, resulting in negligence on the part of the provider. Can proximate cause be established? And how will the suit even be litigated?
Below is a sample of select state data breach notification laws and key provisions that illustrate some of the distinctions between and among state data breach notification laws:

- **Tennessee**\(^{19}\)
  - “Breach of system security” means the unauthorized acquisition of unencrypted material that compromises the security, confidentiality, or integrity of personal information maintained by the information holder.
  - “Personal Information” means first name or first initial and last name plus (i) Social Security number; (ii) driver’s license number or state issued ID number; (iii) account number, credit card number, and debit card number with the PIN or password needed to access the account.
  - Notification should be made at the most expedient time possible and without unreasonable delay.
  - Customers and attorney general may bring civil action for damages or an injunction.

- **Massachusetts**\(^{20}\)
  - Notice to MA resident whose personal information was acquired or used by an unauthorized person or used for an unauthorized purpose.
  - Notice to MA resident when there has been a breach of security.
  - Breach of security: the unauthorized acquisition or unauthorized use of unencrypted data, or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.
  - Also requires notice to the MA Attorney General and the MA Director of Consumer Affairs and Business Regulation.
  - Notification to resident “without unreasonable delay” must include: right to obtain a police report, how to request a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to the consumer reporting agencies.
  - However, notification to the resident shall not include the nature of the breach or the number of residents affected.

---

\(^{20}\) ALM GL ch. 93H, § 3 (2010).
– Notification to state agencies must include: nature of the breach, number of MA residents affected, and any steps taken by the entity related to the incident.

– Personal information: Name with either SSN, Driver's License/ID #, or Account/Credit/Debit # with or without a password to permit access.

• **Georgia**\(^{21}\)

  – “Breach of the security of the system” means the unauthorized acquisition of an individual’s computerized data that compromises the security, confidentiality or integrity of personal information.

  – “Personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number; (B) Driver’s license number or state identification card number; (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (D) Account passwords or personal identification numbers or other access codes; or (E) Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individuals first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

  – Notify in the most expedient time possible and without unreasonable delay.

  – Notify Credit Reporting Agency if involves over 10,000 residents.

• **Arkansas**\(^{22}\)

  – "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

    • "Personal information" means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) Social Security number; (B) driver's license number or Arkansas identification card number; (C) account number, credit card

---


number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (D) medical information.

– Medical Information: means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional

• Notification in the most expedient time possible and without unreasonable delay.

III. HEALTH CARE DATA RISKS AND POTENTIAL LOSSES FOR WHICH POLICYHOLDERS MIGHT SEEK COVERAGE

A. Network / IT Breaches

One of the main types of data breaches is a large-scale network or IT breach. This is typically defined as the unauthorized use or unauthorized access to network software or data. One illustration - a hacker or other entity steals or otherwise gains access to personally identifiable information ("PI") or PHI. This category tends to be applied broadly in terms of the failure to protect confidential information, and can include theft and human error as well.

Such breach is designed to bring a website or system down, prevent customers or users from accessing or using the network, system or information or to gain access to PII or PHI for illicit reasons such as identity theft. Such attacks can result from a variety of causes, such as receipt or transmission of a malicious code that can cause harm devised to trick users into surrendering personal or other information and theft of passwords and human error. Attacks may also do damage to physical hardware, software and data.

A network or data breach is typically an act or event that occurs against the holder of data or party that maintains a system. For example, if something happens that compromises the functioning of a hospital system’s network or network capabilities, that event may be considered a network breach. Likewise, if something happens that compromises the data or information contained on a network, that too would be construed as a network or IT breach.23

23 Studies done show that over 37% of data breaches globally are due to malicious or criminal attacks, 35% are due to a system glitch, and 29% are due to human error. In the United States, those percentages are 41%, 26%, and 33%, respectively.
B. Liability Concerns

A data breach of any sort is likely to create potential liability arising out of an alleged failure to safeguard data, maintain proper safeguards on a system, or take sufficient action to address the breach. For example, if an entity has failed to create an adequate privacy policy, or implement or adhere to the one it has, or failed to maintain or administer an identity theft prevention program or information disposal program, all of these acts or omissions create the potential for liability. And, these concerns are increasing exponentially in the health care realm due to the heightened protective measures concerning sensitive data, as previously addressed herein.

IV. INSURANCE: ARE HEALTH CARE PROVIDERS COVERED FOR DATA BREACHES?

A. Traditional Coverages

In evaluating potential coverage for health care data losses, what is most instructive to date is looking at the existing body of law concerning coverage disputes for (non-health care) data losses under existing policies. Recent health care data loss cases provide further insight. Regardless, and as discussed further below, these cases concerning coverage under traditional policies may decrease in importance if and when policyholders purchase policies specifically tailored to cyber losses, or even health care cyber losses.

1. First Party Losses

First party claims under traditional commercial policies have been for losses related to property damage and business interruption. The losses claimed can be related to a wide range of costs incurred by the insured party. For liability associated with cyber risks, claimed losses might include: the legal and forensics costs associated with investigating a data breach notification and credit-monitoring costs, costs to change account numbers, costs to manage bad publicity, loss to business income arising out of cancelled contracts, loss of new business, data restoration expenses, among other claims. Outside of the health care context, some courts have found that data breaches and/or cyber-attacks may trigger coverage under general commercial liability policies and business interruption provisions.

For example, in *Lambrecht & Assoc. v. State Farm Lloyds*, the court held that an attack by a hacker was covered under the commercial property insurance. In *Lambrecht*, a hacker had used a virus to attack the insured’s computers. The computers froze and some computer data could not be retrieved. The server eventually had to be replaced and a new operating system was purchased. The critical policy provision provided that the, “[insurer] will pay for accidental direct physical loss to business personal property at the premises described ….”. Because the court held specifically that the loss was both accidental, and physical, the question of whether a loss was accidental boiled down to whether or not the insured could have “reasonably anticipated” the loss. The court held in this case that the insured could not have reasonably anticipated the loss. Moreover, it determined that the loss

was “physical,” because the policy language covered “records … exist[ing] on electronic or magnetic media.” Therefore, the losses were covered.

Likewise, in Southeast Mental Health Ctr. v. Pac. Ins. Co., the court addressed business interruption losses. There, a storm caused damage to the Plaintiff’s clinic that resulted in a loss of electrical and telephone service to the clinic. The loss of electricity damaged the clinic’s pharmacy computer, and data was lost. Plaintiff was forced to suspend operations and accordingly lost substantial business income. The insurance provision at issue indicated that the insurer would provide coverage

“For the actual loss of Business Income you sustain due to the necessary ‘suspension’ of your operations during the ‘period of restoration.’ The suspension must be caused by direct physical loss of or damage to property at premises… The loss or damage must be caused by or result from a Covered Cause of Loss.”

Although the court held that the suspension of the Plaintiff’s operations was not “caused by direct physical damage to the property,” it did hold that the Plaintiff’s business losses due to the damage to its pharmacy computer were “caused by direct physical damages to the property.” Notably, the court found that “physical damage’ is not restricted to the physical destruction or harm of computer circuitry, but includes loss of access, loss of use, and loss of functionality.”

While these cases provide examples of when cyber risks may be covered for first party losses, it remains uncertain whether first party claims in a HIPPA context will be covered or whether those types of claims will garner further, and more limiting, analysis. Nevertheless, in light of the constantly changing landscape in the health care area, insureds should not discount the possibility of making first party claims.

2. Third Party Losses

Coverage issues for cyber risks have arisen most frequently in the third party context under an insured’s Commercial General Liability Policy (CGL). Coverage has been sought under either the insuring clause for “property damage” and “bodily injury,” or the clause for “personal and advertising injury.” Under the ISO form definitions, property damage is typically defined as: “physical injury to tangible property” and/or the “loss of use of tangible property that is not physically injured.” Under the ISO form definition, “personal and advertising injury” typically includes coverage for “[o]ral and written publication, in any manner, that violates a person’s right to privacy.”

Property Damage or Bodily Injury

One of the seminal cases for coverage for cyber loss, Eyeblaster, Inc. v. Federal Insurance Company, provides an example of coverage. There, an internet advertising company was sued by a computer user whose computer was allegedly injured, along with his

---

26 See, e.g., ISO Form CG 00 01 10 01.
27 See, e.g., ISO Form CG 00 01 10 01.
28 See, e.g., ISO Form CG 00 01 10 07.
29 Eyeblaster, Inc. v. Federal Insurance Company, 613 Fed 797 (8th Cir. 2010).
software and data, after visiting an Eyeblaster website. Property damages was defined under the relevant provisions of the policy to mean “physical injury to tangible property, including resulting loss of use of that property . . . ; or loss of use of tangible property that is not physically injured.” The Eighth Circuit ruled that Eyeblaster was not covered under the clause in its policy that covers damage to “physical injury to tangible property,” specifically holding that the loss suffered was not “physical injury to tangible property,” because no claim was made for physical injury to the hardware or the user’s computer.

However, because the policy defined “property damage” to include the “loss of use of tangible property that is not physically injured,” the court ultimately found the insured was covered. The court reasoned that the Plaintiff’s computer was tangible property and that since the Plaintiff had alleged that the computer had “froze up” and would “stop running or operate so slowly that it will in essence become inoperable,” that there was a “loss of use.”

**Personal and advertising injury**

With regard to the “personal and advertising injury” insuring clause, coverage is typically extended where there has been “[oral and written publication, in any manner, that violates a person’s right to privacy.” 30 For example, in *Netscape Communs. Corp. v. Fed. Ins. Co.*, the Ninth Circuit found that a personal injury had occurred when Netscape used a product with a feature that sent information to Netscape about its users’ internet activities without their knowledge. This information was used to create profiles of the users. Thereafter, Netscape shared these profiles with AOL (an affiliated entity). The court determined that Netscape’s actions triggered the policy, which defined personal injury offenses as including “[m]aking known to any person or organization written or spoken material that violates a person’s right to privacy.”31

Moreover, it appears that “publication” may include allegations of internal disclosure of data, even if not yet accessed by third parties. *Zurich Am. Ins. Co. v. Fieldstone Mortg. Co*, is instructive.32 In *Zurich*, the court held that the “publication” element of an “advertising injury” claim did not require publication to a third party. There, the allegations involved the use of credit information in order to send individuals prescreened credit offers. The insured was claimed to have improperly accessed and used said credit information upon which the credit offers were made. The court held that “publication”, which was not defined in the policies, should be given its “customary, ordinary and accepted meaning.” Unlike the meaning found in common law tort claims alleging invasion of privacy, publication here was meant to capture less broad based dissemination. The court further noted that of the circuits to examine the issue, the majority do not require publication to a third party for coverage of “advertising injury.”33

Coverage for cyber losses for “personal and advertising” under a CGL policy is certainly not guaranteed. A very recent decision before a Connecticut appellate court, *Recall Total Information Management Inc. v. Federal Ins. Co.*, involving electronic data containing

---

30 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.”


33 See also *Am. Family Mut. Ins. Co. v. C.M.A. Mortg., Inc.*, No. 1:06-cv-1044, 2010 U.S. Dist. LEXIS 2379 (S.D. Ind. Jan. 12, 2010) (unauthorized access of credit reports meets the publication requirement even without publication to a third party).
sensitive personal information belonging to IBM employees, illustrates this point.34 The case
arose after IBM computer tapes fell out of the back of a transportation contractor’s van near a
highway exit ramp. The tapes contained Social Security numbers, birth dates and contact
information for about 500,000 IBM past and current employees. After falling out of the truck
onto the road, about 130 of the tapes were taken by someone and disappeared. However, after
determining that the personal information on those stolen tapes could not be read by a
personal computer, and due to the lack of evidence that anyone had accessed the information,
it was acknowledged between the parties that IBM employees had not suffered injuries from
the loss of the tapes.

IBM contractor, Recall, as an additional insured to its transportation contractor,
sought coverage for the nearly $6.2 million spent for IBM to respond to the breach. The
Recall court determined that there was no coverage because the claim did not trigger the
policy’s coverage for injuries resulting from the “publication” of information that violates a
person’s right to privacy. The court determined that “access is a necessary prerequisite to the
communication or disclosure of personal information….”35 Nevertheless, this case cannot be
viewed as necessarily precluding coverage for such data losses -- including health care
related losses -- under CGL policies. Presumably, the “personal and advertising” injury
provision would be triggered in cases where there is evidence of access to data.36

**Health Care Data Loss**

Very recently, health care data loss was covered under a CGL Policy. In *Hartford
Casualty Ins. Co. v. Corcino & Associates, et al.*, a hospital sought coverage for two class
actions arising out of the alleged disclosure of patients’ confidential medical records when
the information was posted on a public website. The hospital sought coverage under its CGL
policy under the “personal and advertising” injury provision. The insurance company,
however, claimed 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 U.S. District Court for the Central District found for
the hospital concluding 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 data loss was covered.

3. **The Evolution of Coverage for Data Breaches**

As technology advances, the risks associated with such increase and, not surprisingly,
insurance products aimed at such risks continue to evolve. Cyber risks continue to be
funneled into cyber polices and excluded (via endorsements) from traditional policies.38
The evolution of the market, together with the new and heightened cyber risks in health care, highlight the need for health care providers to timely assess the status of their coverage and whether there are dangerous gaps – particularly for large cyber risk claims.

V. DATA BREACH RISKS SPECIFIC TO HEALTH CARE

The cumulative effects of the enactment of both HITECH and the new Omnibus Rule have combined to produce a landscape rife with potential health care industry-specific risk. The new and revised regulations under HIPAA have changed the scope and probability of health care risks and potential liabilities.

The changed landscape means that those in the health care industry, as well as business associates and other entities that may deal with protected data, should evaluate the higher risks of liability in assessing potential coverage. That evaluation should involve more than simply looking at the state of play for cases addressing coverage of data losses generally.

The new Omnibus Rules has increased the risks involved with maintaining and using PHI in several significant ways:

- **Increased fines and penalties.** Penalties have increased up to $1.5 million (annually) for repeat violations, with the potential to exceed $1.5 million if the violations are of distinct.
- **Narrowed defenses to penalties.** Removal of the defense that the covered entity did not know of a violation, or could not have known through reasonable diligence. Further, penalties can now be imposed even if a violation is corrected in a timely fashion, whereas previously penalties could not be imposed unless a violation was due to willful neglect.
- **Broader liability for acts of business associates and subcontractors.** Some estimate that business associates now make up more than 60% of HIPAA violations. Now, Covered Entities can be held liable for the violations of their business associates through the agency relationship even if they were not aware of any pattern and practice of violations, highlighting the increased significance of Business Associate Agreements (BAA’s).

A. Applicable Legal Standards and Insurance Provisions

Three of the chief risks created by HIPAA are investigation costs, fines and penalties, and notification costs. As health care moves forward into the era of electronic health records

---

41 HIPAA Compliance at www.hipaa.com/hippaa-compliance.
42 See 78 Fed. Reg. 5566, 5580. 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 …”
and broad-based data access, coverages under traditional policies will necessarily intersect with these emerging trends causing multi-layered hurdles if the risks are not adequately addressed as part of a facility’s enterprise risk management assessment and program. We already see this intersection, albeit not playing out well for providers, with regard to fines and penalties. Said differently, providers must be careful that fines and penalties are not excluded from coverage.

1. **Insuring Under Traditional Policies.**

In order to obtain coverage under traditional policies for HIPAA “fines” and “penalties,” an entity must assess whether coverage is available for data breaches in privacy violation contexts. A central question should involve the determination of whether statutory “damages” are actually damages, and not fines or penalties, as these terms are defined. This is because fines and penalties are typically the subject of exclusions. As we now know, fines and penalties can be the driving quantitative force in a provider’s loss or claim.

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 Ins. Co. v. Lou Fusz Auto. Network, Inc.*, the court analyzed whether required payments under the Telephone Consumer Protection Act (“TCPA”) constituted damages because the garage liability policy at issue specifically excluded coverage for fines and penalties. The TCPA is a federal statute that prohibits unsolicited fax advertisements and imposes damages of $500 (for each violation). Lou Fusz Auto Network had been sued for sending unsolicited faxes and was seeking a declaratory judgment for both defense costs and indemnity. The court found that the TCPA was meant to be both punitive and remedial, and then went on to conclude that because the payments contained some remedial nature, they were not “penalties,” and it granted coverage for the defense costs.43 With specific regard to fines in the privacy context, in *Visa Inc. v. Certain Underwriters at Lloyds, London*, 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.”44

Traditional policies that cover independent contractors might be used to cover business associates for HIPAA violations. For example, in *Cottage Health System v. Travelers Cas. & Insur. Co*, a California court held that doctors (who were business associates of the hospital), were covered as “independent contractors” under a D&O policy.45 The court determined that the definition of independent contractor was ambiguous (it defined independent contractors as being under the “exclusive direction” of the hospital). This ambiguity was interpreted in favor of the policy holder and the court denied

---

the insurer’s motion for summary judgment. The insurer’s argument was that “independent contractors” should be narrowly construed under the policy to exclude doctors and thus avoid coverage.

**B. Looking Forward: Developing Cyber Policies Geared Towards HIPAA Violations and Provisions**

In light of the significant increase in regulatory oversight of the privacy and security of personally identifiable data, both in and outside of healthcare, insurers are introducing policies specifically tailored to cyber-risks in the health care arena. Notably, these policies provide for coverage of business associates to account for the expanded potential liability under HIPAA faced by business associates. This is particularly relevant because even though many business associates may be storing protected data, and thus subject to health care specific regulations, many remain unaware of the potential risk generated in such a scenario.

The examples provided below attempt to illustrate how insurance carriers are addressing each of the three main risks under HIPAA (penalties, investigation costs, & notifications costs).

**Example #1: Penalties**

Some policies have an expanded definition of “loss” to include HIPAA penalties. For example:

“**Loss**” means damages, judgments (including pre/post-judgment interest on a covered judgment), settlements, and Defense Costs; however, Loss shall not include:

1. civil or criminal fines or penalties imposed by law, **except**:
2. HIPAA Penalties, subject to the HIPAA Penalties Sublimit of Liability set forth under Clause 6 “LIMIT OF LIABILITY (FOR ALL LOSS – INCLUDING DEFENSE COSTS)” of this policy.46

**Example #2: Notification Costs**

Notification costs under the new Omnibus Rule are substantial and likely to increase. To address these costs, certain insurance providers are offering an Information Privacy Coverage Endorsement that they present as specifically tailored to cover HIPAA fees. Such an endorsement can specifically identify notification costs as covered costs. For example:

**HEALTH INFORMATION PRIVACY AND NOTIFICATION COSTS**

*Subject to the Information Privacy aggregate limit of liability stated on the certificate of insurance, we will:*

---

1. Pay “HIPAA” fines and penalties pursuant to the Health Insurance Portability and Accounting Act “HIPAA”, which you become legally obligated to pay arising from a “HIPAA” proceeding with respect to the management and transmission of confidential health information; and

2. Reimburse you for notification costs related to the disclosure of confidential personal information provided that you obtain our prior approval before incurring such costs.

3. Pay claim expenses related to 1. and 2. above.47

This provision specifically provides coverage for those expenses which are incurred while notifying patients of a breach related to protected information.

Example #3: Investigation Costs

Investigation costs have also been addressed by insurance companies. One way this has been done 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 mirror the following:

“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 upon you under the Health Insurance Portability and Accountability Act (“HIPAA”), or any rules or regulations promulgated thereunder, with respect to the management of confidential health information.48

This particular example appears to provide a rather broad definition of a HIPAA proceeding, but could also be constructed to capture even more risk by including defense costs in proceedings brought by state attorney’s general under the HITECH Act.

Judicial construction of these emerging policies is underdeveloped at this point in time.

VI. CONCLUSION

In light of the expanded liability faced by health care organizations and the fact that insurance coverage for relevant losses is in limbo, health care organizations must elevate cyber risk and related losses to the top of their priority list. The failure to do so could result in an unwelcome, and very expensive, cost or expense that detrimentally impacts their bottom line.
