

The Evolving Health Care Cyber Liability Landscape

How Legislative, Regulatory and Insurance Coverage Developments Have Shaped the Unique Exposures Health Care Organizations Face Today

Abstract

The frequency of data breaches and the harm that results from them continue to rise, even though health care organizations are revamping their privacy policies, reviewing their information security protocols and purchasing insurance policies specifically for cyber liability. Breach exposure has increased because of the expanding volume of data that health care organizations must secure and manage; the explosive growth in mobile devices; and the increased information sharing through networks, software applications, electronic health records systems and health information exchanges. Securing protected health information (PHI) has come to the forefront for many health care organizations over the last few years in the wake of settlements and fines, often in excess of $1 million, that have been levied throughout the industry.

This white paper is intended to help readers navigate the current health care cyber liability landscape. It documents how risk is rising, highlights how the Health Information Technology for Economic and Clinical Health (HITECH) Act has dramatically changed liability exposure for health care organizations, identifies additional resources to reduce risk and potential liability for a breach, and explains how a cyber liability insurance policy in conjunction with robust loss control can help mitigate the overall exposure to a data breach in the current legal and regulatory environment.

Risk and Exposure Are Rising

The consequences of data breaches for U.S. health care organizations rose considerably in January 2013 when the HITECH Act became law. Enacted as part of the American Recovery and Reinvestment Act of 2009, the HITECH Act promotes the adoption and meaningful use of health information technology and addresses the privacy and security concerns associated with the electronic transmission of health information. Under the Act, fines for a single incident, once capped at $50,000, could now go as high as $1.5 million for health care organizations (referred to in the regulation as “covered entities”) and their business associates (Figure 1). Furthermore, the director of the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) has promised to “vigorously enforce” the Final Omnibus Rule’s enforcement standards.

Copyright © 2014 AHA Solutions, Inc. - 155 North Wacker Drive, Suite 400, Chicago, IL 60606 | solutions@aha.org | 1.800.242.4677

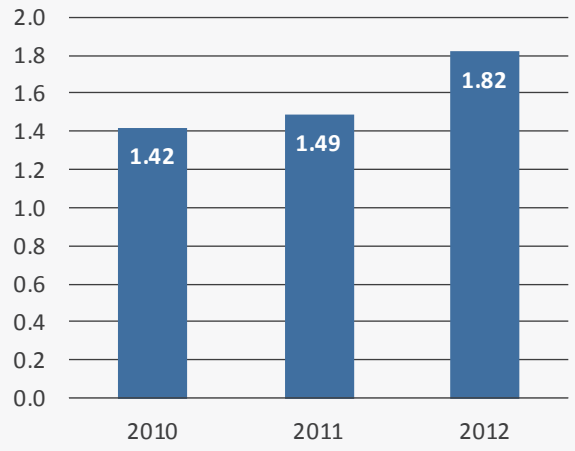
AHA Solutions

Figure 1: HITECH Act Violation Categories and Penalties		
HITECH Act Violation Category	**Allowable CMP for Each Violation**	**Annual Limit per Violations of Identical Provision**
(A) Did Not Know	$100 – $50,000	$1,500,000
(B) Reasonable Cause	$1,000 – $50,000	$1,500,000
(C)(i) Willful Neglect – Corrected	$10,000 – $50,000	$1,500,000
(C)(i) Willful Neglect – Uncorrected	$50,000	$1,500,000

The Act also expands the types of disclosures that need to be reported as breaches. It places the burden of proof on the party that disclosed the information to show that the disclosure was not harmful and thus should not constitute a breach.

Another significant change is that a covered entity's business associates can now be held directly liable for any PHI disclosures they make. That change occurred in January 2013 when the Health Insurance Portability and Accountability Act (HIPAA) was updated via the Final Omnibus Rule (Final Rule). The update brings a health care organization's IT service providers, research partners, billing firms and other contractors under the HITECH Act enforcement umbrella. These firms may not be aware of or familiar with health care data handling regulations and practices, which increases the chances of noncompliance because any impermissible PHI disclosure is now presumed to be a breach.

Figure 2: U.S. Medical Identity Fraud Victims 2010 – 2012 (in Millions)



Sources: Ponemon Institute, First Annual National Survey on Medical Identity Theft, February, 2010: Ponemon Institute, Second Annual Survey on Medical Identity Theft, March 2011: Ponemon Institute, Third Annual Survey on Medical Identity Theft, June, 2012 as presented in the Medical Identity Fraud Alliance report "The Growing Threat of Medical Identity Fraud: A Call to Action" July 2013.

The stronger potential penalties under the HITECH Act and the Final Rule's expanded regulatory enforcement come at a time when health care organizations and their business associates who handle PHI have more exposure to data breaches than ever before. The number of health care records exposed in data breaches rose 1,218 percent in 2012,[i] and there was a 28 percent increase in medical identity fraud victims between 2010 and 2012 (Figure 2). The number of medical identity fraud victims was forecast to rise 19 percent in 2013.[ii] In addition, the health care sector accounted for 43.8 percent of the total breaches on the Identity Theft Resource Center (ITRC) breach list, overtaking the business sector (at 34.4 percent) for the first time since 2005, according to the Identity Theft Resource Center's 2013 Breach Report.[iii]

New Rules, Increased Enforcement

Lack of understanding about HITECH and state privacy law requirements is already creating increased risk for health care organizations. Nearly one-third of the PHI data security problems were attributed to lack of understanding of applicable regulations, according to an audit report from the OCR. Only 13 out of 115 covered entities passed the OCR's initial data security audits, a 90 percent fail rate. With the rules changing, the potential for misunderstanding increases. As OCR Senior Advisor Linda Sanches told[iv] attendees at the 2013 Compliance Institute produced by the Health Care Compliance Association: "You probably don't know what you don't know."

There are plenty of real-world examples illustrating how unfamiliarity with HITECH rules and requirements has led to significant fines and penalties. For example, Walgreens was hit with a $1.4 million judgment in 2013 after losing a civil suit that alleged the company did not adequately train a pharmacist on how to protect patient data. Walgreens' competitor Rite Aid had previously received a $1 million fine from the OCR in a similar case.

The OCR and other regulators are increasing data security enforcement. The U.S. Federal Trade Commission (FTC) has signaled it will become more involved in health care regulation. In August 2013, the FTC filed a complaint against LabMD[v] alleging the testing laboratory failed to reasonably protect patient information. The complaint came after the FTC discovered LabMD had put 10,000 billing records on an inadequately secured file sharing network. The FTC claimed authority to pursue the complaint under Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a) and pursued the enforcement independent of the OCR. Beyond the federal level, nearly every state in the U.S. now has some form of data privacy law that includes breach notification requirements.

Court rulings and regulatory developments in other industries could also have implications for health care organizations' cyber liability exposure. Cases involving retailers and email marketers have helped influence what many courts now find constitutes a breach. In these cases,

Guide to Abbreviations & Acronyms

BA — Business associate
CE — Covered entity
Final Rule — In this paper, Final Rule refers to the HITECH Act Final Omnibus Rule of January 2013
EHR — Electronic health record
HIE — Health information exchange
HIPAA — Health Insurance Portability and Accountability Act
HHS — U.S. Department of Health & Human Services
HITECH Act — Health Information Technology for Economic and Clinical Health Act
OCR — The U.S. Department of Health & Human Services' Office of Civil Rights
PHI — Protected health information

"This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

— Leon Rodriguez, Director
U.S. Department of Health and Human Services
Office for Civil Rights (OCR)

courts have ruled that email addresses and ZIP codes can be considered personally identifiable information.

In 2011, the Securities and Exchange Commission (SEC) issued guidance[vi] that it may be "appropriate" for public companies to disclose whether they have cyber insurance so that investors can properly assess the company's risk profile. The implication is that insurance reduces risk, and therefore companies potentially could be considered negligent for failing to carry cyber insurance. These developments are not specific to the health care industry but are reminders that privacy law is evolving on a shifting foundation across industry landscapes.

In February 2013, President Obama issued an Executive Order (13636) directing the National Institute of Standards and Technology (NIST) to work with critical infrastructure stakeholders, including the health care sector, to develop a voluntary framework for reducing cyber risks. In February 2014, NIST issued Version 1.0 of the framework, including a Framework Profile to help organizations progress from their current level of cyber security sophistication to a targeted improved state. While the Executive Order and Framework Profile help establish a minimum level of security for health care organizations that is currently voluntary, plaintiffs may attempt to utilize the framework to establish a standard of care in connection with cyber liability litigation against a health care organization that is considered to be critical infrastructure.

Technology Risk Factors

Ever-expanding networks and databases and the use of mobile and wireless devices make information easier to share and harder to secure. As the sharing of PHI by various means increases across the health care industry, so does the risk of a data breach exposure.

Tablet computers and other smart handheld devices outsold PCs for the first time in history last year. It is not a coincidence that health care data breaches are rising in frequency at a time when the business use of mobile devices is exploding. Nearly one-half of all health care data breaches result from mobile devices[vii], with lost laptops and smartphones a leading cause.

Lack of encryption and inadequate wireless protection also contribute to mobile device breaches. Health care organizations' IT systems and policies for protecting health care information need to reflect these realities.

Technology creates many types of liability exposure, as the following examples illustrate:

- In 2013, the Hospice of Northern Idaho was fined $50,000 after reporting an unencrypted laptop was stolen and the subsequent OCR investigation determined there had been insufficient risk analysis and policy implementation.[viii] The action is notable because it was the first HITECH Act enforcement involving a breach of less than 500 affected individuals.

- Idaho State University agreed to pay HHS a $400,000 fine in May 2013 based on a breach at a family medicine clinic.[ix] The OCR investigation determined that Idaho State had conducted an incomplete risk analysis and that its server firewalls had been inadvertently disabled.
- Health Net was fined $1.9 million in 2010 after its IT outsourcing service provider reported server drives were missing from a data center.[x] It was also the first company sued by a state attorney general using the expanded enforcement authority of the HITECH Act.
- BlueCross BlueShield of Tennessee received a $1.5 million fine in 2012 as part of a HITECH violation settlement for leaving 57 unencrypted hard drives in an abandoned, leased warehouse.[xi]
- The theft of a portable hard drive without full encryption led to a $1.7 million fine against the Alaska Department of Health & Human Services in 2013.[xii]

The incidents referenced above represent just a small sample of breaches and enforcement actions related to the HITECH Act. From January 2010 through the end of 2013, there were 735 reported breaches affecting 500 or more patients. To help stem the flow of lost and stolen data, health care organizations need to consider some fundamental steps that may help mitigate exposure to a data breach. These steps include:

- Develop and implement an incident response plan (IRP) and regularly evaluate its effectiveness
- Encrypt all portable/mobile devices
- Execute written indemnification agreements with all vendors and third-party service providers that are referred to as “business associates” under HITECH
- Train and continually educate employees and business associates on applicable federal and state laws and regulations to highlight individual responsibility for compliance with the organization’s privacy policies

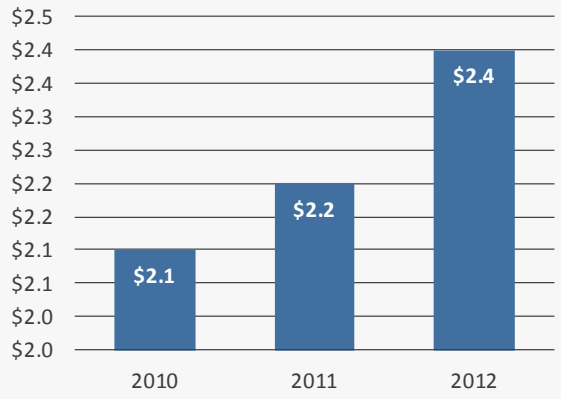
Privacy policy implementation, planning, encryption and ongoing employee education are only the fundamentals of pre-breach preparedness. Organizations must develop specific programs, and evaluate and update them regularly as the flow of information evolves. For example, to date there have only been a handful of breaches stemming from electronic health records and health care information exchanges. As usage of both expands, so will an organization’s cyber liability exposure. Electronic health records accounted for 1.2 percent of all health care breaches in 2012. However, the Memorial Healthcare Systems’ EHR breach that affected 102,153 individuals was the fifth-largest breach of 2012, according to an independent analysis of HHS data.[xiii]

Costs and Consequences Are Rising

The HITECH Act significantly raises the amount of fines that can be levied as a result of a PHI breach, but data breach expenses were rising even before the new penalty schedule took effect. The average data breach cost health care organizations $2.4 million to resolve in 2012, which is 14 percent more than in 2010 (Figure 3). In addition, at $233 per record health care organizations worldwide have the highest per capita data breach cost of any industry.[xiv]

The increase in fines under the HITECH Act is part of the reason costs are rising. Fines, however, only represent a portion of data breach costs. Organizations also need to conduct forensic investigations into the breach, work with investigators and develop remediation plans. Indirect costs such as these account for 68 percent of the total breach cost, according to a Ponemon Institute analysis.[xv] Indirect costs can account for an even higher percentage. For example, Health Net, which was assessed a $1.9 million fine for its missing drive incident, reported spending an additional $7 million on the investigation and follow-up customer support services.

Figure 3: Average Organizational Cost per Healthcare Data Breach 2010 – 2012 (in $ millions)



Source: Ponemon Institute, "Third Annual Benchmark Study on Patient Privacy & Data Security" December 2012.

Cyber Liability Insurance Rounds Out Protection

With the cyber security landscape constantly evolving and risks increasing, health care organizations need to reassess how they protect themselves. Cyber liability insurance is a fundamental risk mitigation tool that health care organizations should consider including in their risk management programs.

The recent increase in both the awareness of cyber liability insurance and its value has been dramatic in the health care industry. In August 2013, only 31 percent of organizations surveyed had already purchased cyber liability insurance but 57 percent indicated that they planned to purchase a policy, according to a Ponemon Institute study.[xvi] The SEC's guidance on the procurement of cyber liability insurance and its potential role as a mitigating factor in enforcement actions is also leading more organizations to make the purchasing decision sooner rather than later.

Conclusion

It's becoming harder for health care organizations to adequately secure PHI because of new regulatory requirements, the widespread use of mobile devices that access PHI, tougher government enforcement and increasingly sophisticated hackers. The landscape is further clouded by changing judicial and regulatory guidance about the very definition of PHI and what minimum risk management controls are appropriate. The effects of these developments are clear — there have been documented increases in the frequency of breach incidents, the volume of records compromised and the costs incurred by violators.

The risks and requirements of health care information management are changing and many organizations need to change in response. Cyber liability insurance, coupled with an incident response plan and the implementation of other risk mitigation best practices, can help health care organizations expand their protection against the increasing risk of a data breach and heightened enforcement in the cyber regulatory landscape.



About AHA Solutions

AHA Solutions, Inc. is a resource to hospitals pursuing operational excellence. As a subsidiary of the American Hospital Association, AHA Solutions collaborates with hospital leaders to identify key challenges the field faces. After conducting the proprietary *AHA Signature Due Diligence Process*™, we award the exclusive AHA Endorsement. As an AHA member service, AHA Solutions provides access to content experts and education to support product decision making, and convenes people with like interests for knowledge sharing that is centered on timely information and research.

AHA Solutions is proud to reinvest its profits in the AHA Mission: To advance the health of individuals and communities. For more information, contact AHA Solutions at 800.242.4677 or visit www.aha-solutions.org.

About Chubb

CyberSecurity by Chubb for Health Care organizations has been awarded the exclusive AHA endorsement. The member insurers of the Chubb Group of Insurance Companies form a multi-billion dollar organization providing property and casualty insurance for personal, commercial and specialty lines customers worldwide through 8,500 independent agents and brokers. Chubb's global network includes branches throughout North America, Europe, Latin America, Asia and Australia. For more information visit www.chubb.com.

Actual coverage is subject to the language of the policies as issued. This document is advisory in nature. It is offered as a resource to be used together with your professional insurance advisors in maintaining a loss control program. No liability is assumed by the information contained in this document. Chubb refers to the member insurers of the Chubb Group of Insurance Companies. Chubb, Box 1615, Warren, NJ 07061-1615.

[i] NetDiligence “Cyber Liability & Data Breach Insurance Claims; A Study of Actual Payouts for Covered Data Breaches” October 2012.

[ii] Ponemon Institute “2013 survey on Medical Identity Theft” September 2013.

[iii] Identity Theft Resource Center “2013 ITRC Breach Report” March 24, 2014.

[iv] As quoted by Modern Healthcare April 23, 2013: http://www.modernhealthcare.com/article/20130423/NEWS/304239958/audits-find-organizations-unaware-of-new-data-privacy-rules.

[v] U.S. Federal Trade Commission “FTC Files Complaint Against LabMD for Failing to Protect Consumers’ Privacy” August 29, 2013. http://www.ftc.gov/opa/2013/08/labmd.shtm

[vi] Division of Corporation Finance Securities and Exchange Commission “CF Disclosure Guidance: Topic No. 2 Cybersecurity” October 13, 2011.

[vii] Ponemon Institute “Fourth Annual Benchmark Study on Patient Privacy & Data Security” March 2014.

[viii] US Department of Health & Human Services, “Case Examples and Resolution Agreements,” www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

[ix] U.S. Department of Health & Human Services “Idaho State University Settles HIPAA Security Case for $400,000” May 21, 2013, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement-press-release.html.html.

[x] Foley Hoag LLP, “Security, Privacy and the Law”, Connecticut Attorney General Reaches First State HIPAA Settlement with Health Net

[xi] HHS Settles HIPAA case with BCBSTN for $1.5 million, http://www.hhs.gov/news/press/2012pres/03/20120313a.html.

[xii] Alaska Settles Securities Case for $1,700,000, http://www.hhs.gov/news/press/2012pres/06/20120626a.html

[xiii] Redspin “Breach Report 2012: Protected Health Information” February 2013.

[xiv] Ponemon Institute “2013 Cost of a Data Breach Study: Global Analysis” May 2013.

[xv] Ponemon Institute “2013 Cost of a Data Breach Study: United States” May 2013.

[xvi] Ponemon Institute “Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age” August 2013.