Bloomberg Law Reports® Privacy & Information

Why the Time for Security & Privacy Insurance Has Arrived

Elizabeth G. Litten and Mark G. McCreary, Fox Rothschild LLP

You may think that a $30 USB drive does not seem like the most costly business asset you could lose, but you would be wrong.

Protected personal information (PPI) and protected health information (PHI) lurk in almost every business. Employee information, including IRS W-4 forms, health questionnaires, payroll and financial information fill file cabinets and computer hard drives across the country. Businesses often keep such information about individuals even when they have not been employed by the company for decades. Customer information, such as personal and financial information, fill CRM databases, e-mail archives and smartphones in every state (and every country, in the case of traveling employees practically or physiologically unable to leave the smartphone at home). Even user information for online access to accounts, features and services permeate a substantial portion of modern businesses, with troves of full names, home addresses, credit cards and mother's maiden names stored in redundant databases, including those floating in that magical place referred to as "The Cloud."

Conscientious risk managers have known for decades that locked filing cabinets, restricted off-premises access and only-as-necessary employee and vendor access to paper files are best practices. Most businesses are now familiar with the risks associated with electronic data storage of PPI and PHI and have implemented policies and systems to prevent unauthorized access and data breaches. Encrypted transmission of PPI and PHI has been the norm for most savvy businesses for years, and encrypted storage is slowly trickling down to even smaller businesses.

PHI is often the data that when set loose in the wild creates the most startling and damning headlines. It is a fact of life in 2011 that hospitals and other health care providers and payers (health insurance carriers and other types of health benefits plans) must maintain, record and transmit PHI electronically. Transmission of PHI electronically does not stop within the walls of the business or even across secure intranets for providers with multiple locations. Transmission involves the submission of claims to government or third-party payers, sharing information with other health care providers and communicating with patients and their families.

An example of how far reaching a "transmission" can be is found in the proposed regulations from the Department of Health and Human Services, Office for Civil Rights (OCR). Under the proposed regulations, "electronic" health information transmissions include even those transmissions on paper, by facsimile or on a voice mail message, if the information being exchanged existed in electronic form before the transmission took place.[1]

By way of analogy, if we apply the foregoing proposed regulation to banking information, if an account manager calls her client and leaves a voicemail regarding confirmation of a securities purchase for account no. 8164540774, she would need to be certain that access to the voicemail is limited to the authorized persons, nobody intercepted the call and at all times the transmission, access to and storage of the voicemail was encrypted. There is no doubt that best practices dictate that the account manager should have never left a voicemail with such detailed information, but the point is there is arguably no regulation preventing the account manager from leaving the voicemail message. Back to the medical context, even those providers that are slow to implement electronic health records (EHRs), and vendors of providers that do not view themselves as coming into contact with PHI, have legal obligations to recognize and secure it under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) laws and implementing regulations.

While a major concern already for hospitals and other health care providers as well as for payers and others whose business involves health care, the creation, transmission and storage of PHI and PPI should also be a concern for other types of businesses. Treatises have been written, and millions, if not billions, of corporate dollars have been spent, on the subject of handling and storage of PPI. The time and dollars spent on the actual formulation of policies and the handling of PPI by businesses grows every year, as requirements become stricter and more widespread. However, experience has taught businesses that no amount of prevention, protection and security can guarantee data is secure. Disgruntled and rogue employees, corporate espionage and a bored 12-year-old in Bulgaria are constant threats to any business with PHI or PPI that has any value on the black market or is a target for embarrassment in the media. It is often not the wild scenario of Ethan Hunt stealing the NOC list in "Mission Impossible" that creates the greatest risk of PHI or PPI loss or theft.

Consider the following examples. A personal wealth manager's car is broken into, and his laptop containing the unencrypted usernames and passwords for online brokerage accounts is stolen. The CFO of a cutting-edge gene therapy company loses her keys, which includes a keychain thumb drive containing unencrypted genetic profiles of all 140,000 customers of the company. The CEO of a social media site has his laptop routinely confiscated by Homeland Security when returning from business trips abroad—his laptop contains unencrypted account information for every user of the social media site, including credit card information used to verify users' identities—and Homeland Security promptly loses the laptop. On one hand, none of the people in the foregoing examples did anything malicious. Yet, none of the information should have been accessible by a third party and, under any competent security policy, the unencrypted storage of that data would have been prohibited.

The events leading up to the loss of PHI or PPI are wholly irrelevant. It is the loss itself that creates the problem for the business that experienced the loss. Currently, in addition to HIPAA and HITECH—the federal breach notification laws applicable specifically to PHI—46 states, the District of Columbia, Puerto Rico and the Virgin Islands all have breach notification laws applicable to PHI and/or PPI. The residency of each person contained in the PHI or PPI loss will determine which law(s) apply, meaning it is likely a business would be dealing with several states' laws. There are variations among state laws, such that in some states you must notify the consumer within a set amount of time, while other states require you to contact law enforcement prior to notifying the consumer. It is rare that a business will be able to merely issue a *mea culpa*, purchase credit-monitoring coverage for affected persons and be back to business as usual. Rather, businesses will find rapidly mounting legal bills, public relations strategy decisions and compromises, and class action and private lawsuits in multiple states. In some cases, the costs associated with preparing, implementing and following the requisite data storage and handling policies, including hardware and software costs that should have been in place prior to the data loss, can be crippling because of the suddenness and all-at-once necessity.

If a business provides or pays for health care, "unsecured" PHI lurks among or alongside its PPI. Under HIPAA, PHI includes any "individually identifiable health information," and unsecured PHI exists wherever there is documentation of patient information, whether related to past, present or future conditions, services or items, and includes handwritten and oral notes. Any information connected with an identifying fact about a patient (patient's name, address, telephone number, address, Social Security number or e-mail address, to name a few), or any information that could be linked with an identifying fact about a patient (an accident reported in the newspaper, for instance) may be or create unsecured PHI. If this information is accessed, or could be accessed, by unauthorized individuals or entities, the HITECH breach notification requirements and potential civil monetary penalty provisions will apply.

The late-adopting, low-tech providers and unaware vendors may be less aware of these legal obligations and the potential costs associated with a PHI breach, but they are no less likely to face a PHI breach. In fact, a number of very sophisticated nationally recognized hospitals and esteemed educational institutions have recently had to deal with lapses in their privacy and security policies and procedures that resulted in breaches of PHI. Several recent examples include the Yale School of Medicine, the University of Rochester, the Henry Ford Health System, and the University of Tennessee Medical Center.[2] Undoubtedly, these entities incurred significant costs in terms of the breach notification requirements alone.

On February 14, 2011, the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") settled with the General Hospital Corporation and Massachusetts General Physicians Organization, Inc. over a loss of protected health information that includes a payment to the U.S. government of $1,000,000 by Massachusetts General Hospital for potential violations of HIPAA.[3] On February 4, 2011, HHS imposed a $4.3 million civil monetary penalty assessment (CMP) on Cignet Health and its affiliates (Cignet) for violations of the HIPAA Privacy Rule, including failure to provide patients access to their records and failure to cooperate with an investigation [4]. This is the first time that the OCR has publicized its activities in enforcement actions involving heavy monetary payments. Until now, the publicized enforcement activity for monetary recoveries from covered entities under HIPAA/HITECH has been by attorneys general in Connecticut, Indiana and Vermont.

Unlike the handling of PPI, the loss of PHI is covered by the federal HIPAA and HITECH laws and regulations, that contain (relatively) clear direction and response parameters in the event of a breach. However, the preemption provisions of HIPAA contemplate that more restrictive state laws not "contrary" to HIPAA can complement the HIPAA requirements. Therefore, organizations facing a PHI breach or loss must still conduct an analysis to determine if the data breach law of a particular state includes medical information in its definition of PPI (and many do).

Under the HIPAA and HITECH laws and regulations, entities must provide written notification by first-class mail to all affected individuals or, where the individual has agreed to electronic notice, by e-mail, and must provide a description of what happened. The description is to include the date of the breach and date of the breach discovery, if known; a description of the types of unsecured PHI involved in the breach; information regarding steps the entity is taking to investigate the breach, to mitigate harm to the individuals and to prevent further breaches; as well as contact procedures for individuals to ask questions and get additional information. These contact procedures must include a toll-free telephone number, an e-mail address, a web site or postal address.

With respect to PPI data breaches, the Identity Theft Resource Center identified 498 breaches in 2009, exposing more than 222,000,000 records, as compared to 656 in 2008, exposing more than 35,000,000 records, and representing a 47 percent increase from 2007. Additionally, the average cost of a data breach in 2009 was $204

per affected consumer, as compared to $202 per affected consumer in 2008, and representing a 40 percent increase from 2005. While these numbers only include reported breaches, which likely makes the numbers very misleading about the scope of breaches, and the cost per affected consumer is an average, it does not take a great deal of imagination to multiply the costs by 5,000, 10,000 or 50,000 affected consumers.

In its Aug. 24, 2009, rule proposal, OCR estimated the cost implications associated with various PHI breach notification and contact requirements. It estimated the cost of setting up a toll-free telephone line for a breach affecting the PHI of between 10 and 500 individuals by assuming that a breach of this magnitude would generate 1,772 calls, whereas a breach affecting 500 or more individuals would generate 2,887,032 calls. It then calculated the set up, calling charge and labor costs per call and estimated a breach affecting 10 to 500 individuals would cost $5,067, whereas the cost associated with the toll-free line for breaches affecting more than 500 individuals would be $8,228,041. Clearly, even if one finds fault with OCR's estimates and assumptions, the financial implications of a PHI breach are significant – even before considering potential costs associated with such things as civil monetary penalties, indemnification and damaged reputation.

Knowing that most business have PPI and/or PHI, that policies and safeguards must be in place, that no amount of policies and safeguards will guarantee a breach- or loss-free existence and that the costs associated with a data breach or loss can be astronomical, the question of what can a business do to offset the potentially catastrophic effects of a data breach or loss becomes paramount.

Those persons most cognizant of the potential for breaches and their effects have observed the relatively recent proliferation of "cyber insurance" policies, also sometimes referred to as "Security and Privacy" (S&P) liability coverage. S&P policies have been developed to cover the some or all of the out-of-pocket expenses incurred in connection with data breaches and losses, and may make a lot of sense in light of our increasingly data-driven, electronically communicating world.

S&P insurance policies may cover a wide variety of expenses related to PPI and PHI breaches. The coverage may include protection for the entity not only in terms of the PPI and PHI breach notification costs, but may also cover some or all of the costs associated with the investigation needed to determine the cause of the breach, costs to restore or recollect the breached information, costs associated with public relations and crisis management related to the incident, legal costs, compensatory damages, criminal reward funds and costs associated with mitigating harm to affected individuals.

One S&P insurance carrier (Chartis) provided the following examples of amounts actually paid in connection with PHI and related privacy breaches:

- Employee of a credit union sold information to outsiders. Total amount paid on the S&P policy for liability claim and first party loss: $1,800,000
- Employee stole information and sold it to an identity theft ring. Total amount paid on the S&P policy for notice and liability claims: $2,600,000
- Employee of a medical provider stole and sold more than 40,000 patient records containing PHI. Total amount paid on claims pursuant to the S&P policy covering notification costs: $675,000
- Entity/insured lost tapes containing medical information and Social Security numbers. Total amount paid on the S&P policy covering call center services and credit monitoring of affected individuals: $400,000+

Another carrier (NAS E-MD™; NAS MEDEFENSE™ Plus) provided several real-life examples of S&P loss scenarios particular to health care entities and PHI. This carrier offers "privacy breach response coverage" that includes legal fees, information technology forensic costs, postage costs, advertising costs, public relations expenses, credit monitoring expenses, identity theft education and assistance expenses and call center expenses. Examples of claims paid include:

- Hospital fined by the state for failing to report a PHI breach of 532 patients' medical records within five days after the breach occurred. The state determined an unauthorized employee removed a computer containing PHI; as soon as the hospital determined the computer was unrecoverable, it reported the incident. Actual amount paid by the S&P carrier: $250,000+
- Hospital sued by Patient A after Patient B (a pregnant drug addict) stole Patient A's medical identity and delivered a baby testing positive for illegal drugs. Social workers subsequently attempted to remove Patient A's four children from her, thinking she was a drug addict, and Patient A incurred legal costs to keep her children. Actual amount paid by the S&P carrier: $1,200,000 (damages) and $80,000 (defense costs)
- Pharmacy sold a computer to a private individual; the computer contained prescription records including names, addresses, Social Security numbers and medication lists of pharmacy customers. Total amount paid by the S&P carrier: $410,000+

"An ounce of prevention" may, indeed, be worth "a pound of cure" in the PPI and PHI privacy and security context. Written data storage and handling policies and systems to prevent unauthorized access and data breaches and losses (which must be effective and dutifully implemented and should be frequently tested) are an absolute necessity for a business of any size and for anyone who "touches" PPI and PHI. In the context of hospitals and other health care organizations, it is easy to make the argument that S&P insurance policies also are an absolute necessity. Nevertheless, businesses and providers of all sizes should analyze the realities of increasing cyber crime and the rapidly expanding use of and access to various modes of electronic communication in measuring the relative economic costs and benefits of the added protection of an S&P insurance policy.

Elizabeth G. Litten is a partner at Fox Rothschild LLP and is part of the firm's Health Law Practice Group. She can be reached at (609) 895-3320 or elitten@foxrothschild.com. Mark G. McCreary is a partner at Fox Rothschild LLP and is part of the firm's Media, Defamation and Privacy Law Practice Group. He can be reached at (215) 299-2010 or mmccreary@foxrothschild.com.

---

[1] 75 Fed. Reg. 40868, 40913 (July 14, 2010) (proposed amendment to 45 C.F.R. 160.103): "Electronic media means... (2) Transmission media used to exchange information already in electronic storage media... Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form before the transmission." (Emphasis added.)

[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

[3] http://www.hhs.gov/news/press/2011pres/02/20110224b.html

[4] http://www.hhs.gov/news/press/2011pres/02/20110222a.html (See also *HHS Imposes $4.3 Million Penalty for HIPAA Violations*, Bloomberg Law Reports - Privacy & Information, (March 2, 2011)).