Healthcare industry

The evolving risk of network security and data privacy in the healthcare industry

According to the World Privacy Forum, stolen medical information is worth $50 on the street versus $1 or $2 for a Social Security number (SSN).1 A health record is more valuable because it can be used to access prescription drugs, pay for treatment, or submit false or inflated medical claims. Multiply the number of health records your organization has by $50 and you’ll quickly see why the healthcare industry has emerged as one of the most attractive and lucrative targets for identity thieves.

Between 2011 and 2013, 701 healthcare providers disclosed privacy breaches,2 and the risk is growing, exacerbated by the growing automation and adoption of electronic health records (EHRs), rapid changes in the healthcare delivery system, and millions of new patients entering the healthcare system as a result of the Affordable Care Act. Further, evolving data breach requirements and regulations at the federal and state levels will likely lead to increased fines, enforcement actions, and litigation.3

Data breaches not only threaten providers’ reliability and resiliency, but could also result in significant financial losses. Consider these recent examples of breaches at healthcare organizations:

New York-Presbyterian Hospital and Columbia University (NYP and CU). In September of 2010, NYP and CU submitted a joint breach report to the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) regarding the disclosure of the protected health information (PHI) of 6,800 individuals, including patient status, lab results, vital signs, and medications. Due to the lack of technical safeguards, the deactivation of a personal server on the NYP and CU shared data network resulted in PHI being accessible on internet search engines. In May of 2014, NYP and CU agreed to pay the OCR a combined amount of $4.8 million to settle charges that they potentially violated HIPAA rules. In addition, both institutions agreed to “a substantive corrective action plan, which included undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports.” The combined monetary assessment is the largest HIPAA settlement to date.4

---

AvMed. In late 2013, AvMed settled a $3 million class action lawsuit related to the December 2009 theft of two unencrypted company laptops, which contained personal information — including names, addresses, SSNs, and medical data — on 1.2 million AvMed members. The settlement was unique, as it awarded the plaintiffs regardless of whether they suffered identity theft or not. The agreement required AvMed to pay impacted customers $10 for each year they paid premiums prior to the theft, with a maximum of $30. The settlement explained the amount as a refund of premium overpayment — what AvMed should have spent on data security. In addition, customers who suffered identity theft as a result of the breach could also claim reimbursement from AvMed.

Concentra Health Services. In April of 2014, Concentra agreed to pay the OCR more than $1.7 million to settle potential violations of HIPAA rules, as well as adopt a corrective action plan to evidence their remediation of OCR findings. The settlement stemmed from an OCR compliance investigation initiated in 2011, when Concentra reported the theft of an unencrypted laptop from its Springfield Missouri Physical Therapy Center facility. The OCR found that while steps were taken to begin encryption, “Concentra’s efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization.” The investigation further found that Concentra had insufficient security management processes in place to safeguard patient PHI.

The responsibility to protect private data

The regulatory environment, both at the state and federal levels, has evolved significantly over the past few years. Government agencies are becoming more proactive in their requirements and enforcement actions pertaining to safeguarding PHI.

The 2013 modifications to the HIPAA Omnibus Rule, for example, include various new requirements for healthcare organizations collecting, storing, and processing PHI, as well as standards for use and disclosure of PHI with business associates. Effective September 22, 2014, covered healthcare organizations must bring all of their Business Associate Agreements (BAAs) into compliance with the Rules.


At the state level, data breach notification laws continue to evolve, further requiring healthcare organizations with personally identifiable information (PII) and PHI to comply with numerous, sometimes conflicting, requirements. The variations in state notification laws pose challenges for healthcare organizations that operate in multiple states. To ensure compliance, it is critically important for healthcare organizations and business associates to continually monitor the changing regulatory landscape and maintain updated breach response plans.

Solutions

Wells Fargo Insurance has the experience, knowledge, and market relationships to help your organization implement a comprehensive strategy to manage technology, network security, and privacy liability. Our Technology, Privacy, and Network Risk (TPN) professionals will collaborate closely with you to help identify and reduce risks associated with:

- Collecting, handling, or storing patient, customer, employee, and other confidential information
- Disseminating information electronically
- Classification of data assets
- Data breach preparedness, incident response, and crisis management

We begin by evaluating your company risk profile and then tailor an insurance program to address your specific needs. Comprehensive risk transfer programs typically include protection for:

- Network security and privacy liability
- Network extortion
- Electronic media liability
- First-party business income loss and electronic data restoration expenses
- Regulatory defense, fines, and penalties
- Payment card industry (PCI) penalties, fines, and assessments
- Consumer redress funds

We have worked closely with leading insurers to develop proprietary endorsement language, expanding the coverage offered under a standard policy.

Your organization’s bottom line can also be affected by the costs incurred as a result of a breach event — including legal and forensics expenses, public relations, consumer notification, credit monitoring, and medical identity restoration, which is increasingly relevant for healthcare organizations. With proactive planning, these expenses can be offset by your insurance program.

Wells Fargo Insurance also offers a host of data breach management tools to help manage risk, including incident response planning, educational content, and access to technical resources to assist in the education, prevention, and mitigation of breach events.
How can we help?

For more information on this topic, contact your local Wells Fargo Insurance sales executive, or visit us at wfs.wellsfargo.com.