KAYE | SCHOLER

Hospitals Lag Far Behind Other Industries in Privacy and Data Security

Healthcare institutions should emulate "best of breed" privacy polices developed by financial services firms rather than other hospitals, says Kaye Scholer technology attorney William A. Tanenbaum

April 24, 2013

NEW YORK—When it comes to privacy and data security, healthcare institutions face tremendous exposure to regulatory violations and monetary damages, according to Kaye Scholer Partner William (Bill) Tanenbaum, who advises clients on a wide range of technology and IP issues, including data security and privacy.

"Criminals pay more for stolen personal health information than they do for stolen credit card information. The top of a medical chart contains all the information needed for identify theft," explains Tanenbaum. "While better IT is the solution" he says," not all wheels have to be reinvented. Hospitals and other healthcare institutions that use each other's systems as models may not find them all that effective. Rather they should adopt the IT solutions, privacy and data security procedures and employee education programs that already have been developed and tested by leading financial institutions to protect sensitive personal information in a regulatory environment."

The numbers would seem to support Tanenbaum's claims. According to a recent study on patient privacy and data security, conducted by the Ponemon Institute, 94 percent of healthcare organizations surveyed suffered at least one data breach in 2011 and 2012, with 45 percent of these organizations actually experiencing more than five data breaches during the same period. Lost devices, employee and third-party error, criminal attacks and technology glitches were listed as a few of the leading causes for the breaches, which Ponemon estimated could be costing the US healthcare industry an average of $7 billion annually.

According to an April 2013 ITRC Breach Report by the Identity Theft Resource Center, in the first three months of 2013 alone, the medical and healthcare sector experienced 58 breaches, or 40 percent of all breaches reported in the US (a total of 562,577 compromised records with an astounding 63 percent of them lost). By contrast, ITRC found that so far in 2013 the financial services industry experienced seven breaches, or only five percent of all reported data breaches, for a total of 14 records compromised and with no records actually lost.

"Customers rightfully worry about protecting sensitive financial information such as social security numbers, and checking and credit card accounts," says Tanenbaum. "But healthcare data in many ways can be viewed as even more sensitive because electronic medical histories, laboratory tests and prescribed medicines, if compromised, could harm patient health."

Why are hospitals so technologically unhealthy? According to the Poneman survey, 73 percent of healthcare organizations cited insufficient resources to prevent and find data breaches. In response to this, Tanenbaum says an ounce of IT prevention is worth a pound

Related Lawyer

William A. Tanenbaum

Practice Areas

- IP & Technology Transactions
- Social Media

Related Office

New York

of cure. “Hospitals that fail to commit the necessary technology resources to secure systems up front may face exponentially larger costs in the event of a security breach,” he warns.

The Ponemon study further found that 91 percent of hospitals surveyed reported that they are using cloud-based services to store patient information and records, for both health and financial data. However, 47 percent of the healthcare organizations surveyed reported they lacked confidence in the security of cloud storage. According to Tanenbaum, “this illustrates that cloud computing can be both a benefit and a problem. On the one hand, it lets doctors use iPads to have real-time patient information as they conduct their rounds. On the other hand, off-the-shelf cloud services come complete with privacy risks. The solution is to follow an outsourcing model to provide more robust data security.”

In terms of specific steps that hospitals should take to solve rather than create data security problems, Tanenbaum recommends the following:

- **Hack Your Own System**. Test the strength of your IT and data security systems to find and fix potential problems before criminals and hackers exploit them.
- **Keep Storms Out of Your Cloud**. Chose the right data protection protocols before you send data to the cloud, and use even more careful planning if you use cloud as computation platform as well as a data storage system.
- **Investigate Your IT Vendors**. Ensure that they understand that HIPAA and HITECH regulations are not ordinary business requirements and that your vendors will be effective partners if you have to implement your database breach remediation plan. Make sure the vendors will keep key personnel assigned to your account.
- **Use Checklists for Data Health**. Healthcare workers should follow checklists to ensure data health and protect against computer viruses in the same way that medical staff follows checklists to ensure patient health and prevent infection.
- **Encrypt But Verify**. Encryption provides security, but only if used consistently and as designed.
- **Audit and Then Audit Again**. Ensure that each link in the chain of electronic record collection, storage, analysis and transmission is secure, and that carefully crafted procedures are followed consistently.

William A. Tanenbaum focuses on IP, IT and technology transactions and counsels companies on compliance and legal issues relating to implementing, upgrading and outsourcing IT systems and the legal ramifications that newer technologies such as cloud computing, social media, electronic health records and Big Data have on data security and privacy protection. He has particular experience working in healthcare IT with pharmaceutical companies, biotech firms and other life sciences-related entities. Recently named as New York’s 2013 Information Technology Lawyer of the Year by *Best Lawyers in America*, as well as a 2012 Life Sciences All-Star by *Euromoney*’s Legal Media Guide, Tanenbaum is a past President of the International Technology Law Association and currently serves as a Vice President of the Metropolitan New York Chapter of the Society for Information Management (SIM), an industry association for CIOs and senior IT executives.

About Kaye Scholer LLP
Founded in New York in 1917, Kaye Scholer combines the continuity and business acumen of a century-old law firm with a forward-looking, tech savvy, results-driven approach focused around lasting client relationships. With industry strengths in life sciences, financial services, technology, real estate and energy & infrastructure, Kaye Scholer offers strategic guidance and legal services to public and private entities facing litigation, transactional or governance challenges. Kaye Scholer’s lawyers regularly advise on matters across multiple legal jurisdictions, including in the US, Canada, UK, EU, China and Japan.

###

Contacts:
Sandi Sonnenfeld
PR & Communications Director
212.836.8273
sandi.sonnenfeld@kayescholer.com

Tania Zamorsky
PR & Communications Manager
212.836.8339
tania.zamorsky@kayescholer.com