Washington Healthcare News®
wahcnews.com
Articles, Interviews and Statistics for the Healthcare Executive

A Guide to Cyber Liability for Health Care Industry Employers

By Spencer Hamer
Partner
Michelman & Robinson, LLP

As use of electronic health care records (EHRs) has become increasingly standard, the health care industry is finding itself under siege from cybercrime attacks. Three of the six largest data breaches in 2011 transpired in the health care industry. According to the Identity Theft Resource Center, in 2013, almost half of the identify theft breaches it identified were in the health care industry.

These thefts can have dire implications—a health care data breach substantially increases the risk of data-related fraud. And the value of stolen EHR data is significantly greater than that of a credit card or bank account number, because it can plague a victim for a lifetime, with hackers often using the information in multiple capacities to commit fraud or identity theft. Thousands of recent accounts of unauthorized disclosures of protected health information attest to this fact. Despite the recent Target data breach, financial services and retail operations have been more vigilant about preventing and responding to these threats than have health care industry employers.

In addition, HIPAA and similar regulations place stringent requirements on health care industry employers to safeguard the privacy of patient and medical data. And because EHRs contain so much private data, their existence makes health care employers an enticing target.

A health care organization's employees or ex-employees are frequently responsible for cybercrime attacks. In fact, recent studies suggest that internal health care breaches compromise far more sensitive data than do external incidents.

The bottom line is that health care employers must institute comprehensive security procedures to mitigate the risk of a cybercrime breach. Fortunately, they have a variety of tools at their disposal to do so.

Conduct Thorough Screening: It is critical to identify potential problem employees before they are hired. Examine applications for work history gaps and reasons given for leaving jobs. Check references, going beyond those provided if possible. Consider using background checks and pre-employment testing, but only to the extent permitted by applicable law, including the EEOC's recent guidance memorandum on the use of background checks.

Use the "Broken Windows" Approach: In the 1990s, New York City crime rates dropped

dramatically after the NYPD implemented the "broken windows" theory of preventing crime: cracking down on little offenses to prevent big ones. Employers should have a zero-tolerance policy prohibiting misconduct, including theft, and consistently apply it. If a popular supervisor takes office supplies home, overnight security is lax, and no computer monitoring policy exists, employees will perceive that the company turns a blind eye to security issues, and will act accordingly.

Consider Monitoring Options: Information technology provides employers with a host of options to detect misconduct. For example, computer screens can be monitored remotely. In addition, employees often forget that email communications can be retrieved, even after they have been deleted. And, by setting computer backup systems to preserve information, employers can often obtain "smoking gun" evidence. Work with an IT professional to develop procedures that make sense for your environment. Do routine sweeps to make sure employees are not trying to access confidential electronic records. But consult legal counsel first to evaluate potential restrictions under applicable law. Numerous legal issues arise from monitoring, and lawsuits are being filed on a class action basis for actions such as alleged improper monitoring of telephone calls.

If You Monitor, Give Clear Notice: The employee handbook should make it clear that, to the extent permitted by applicable law, the employer reserves the right to inspect property, including computers, emails, and voicemails on the employer's system, for any legitimate business purpose, without notice or employee consent. It should also indicate that employees have no expectation of privacy in the workplace, and that passwords and login devices do not create a privacy right. In addition, it should make it clear that all information pertaining to the employer and its clients is strictly confidential. Employees should also be cautioned about disclosing information online, including on social networking websites, so having a robust social media policy is also important.

Conduct a Thorough IT Audit: Health care security experts can be retained to thoroughly audit cyber security. One well-known security expert recently recounted how, after being retained by a high-priced Los Angeles hotel with frequent celebrity guests to audit the hotel's new security system, she was able to hack into the system in under thirty minutes and access confidential information. Given the speed at which hacking and other cybercrime techniques evolve, such audits should be conducted at frequent intervals.

Develop Investigation Protocol: A protocol for prompt and thorough workplace investigations into potential theft issues must be established. Among other things, it should identify the persons responsible for investigating and explain the steps in the investigation process. Managers should be regularly trained on the protocol.

Encourage Reporting: Employers should encourage reports of misconduct. Employees, however, are often reluctant to report misconduct, especially when they lack hard evidence. The employee handbook should set forth guidelines on how to report suspected impropriety. Consider using an anonymous reporting service, such as an (800) hotline, and designating an ombudsperson to receive complaints confidentially. Assure employees, through a written policy, that the employer will not retaliate against them for good faith reports of misconduct, regardless of the outcome of the investigation. Consult legal counsel regarding applicable whistleblower protection laws.

Prepare for Public Communications: The public may learn about matters the employer would like to keep confidential. If a cyber theft issue becomes public, employers can exacerbate the problem by appearing defensive, secretive, confused, or uncaring. Moreover, they risk defamation suits if communications are not vetted. Management needs to present a clear, consistent message, and using the proper tone is critical. Designate and train a spokesperson, and for particularly sensitive situations, or if media scrutiny is an issue, consider retaining a consulting firm that specializes in crisis management.

Data Compliance: State and federal laws, including HIPAA and the Affordable Care Act, require medical practices and health care organizations to not only utilize electronic data, but to ensure that the data is secure. Any company that maintains private personal or financial information on patients has the responsibility to protect that information. Any unauthorized release of information or outside breach could violate privacy laws and expose the employer to a

lawsuit. Make sure that you are fully data compliant, and that your information is protected and secure.

Educate the Workforce: Educating your leadership and staff about state and federal privacy laws and HIPAA requirements, and integrating such information into employee handbooks, orientation, and training is crucial. Employers should perform a cyber-risk assessment to make sure employees are not failing to log out when leaving work, sharing passwords, leaving confidential information on their screens, leaving laptops where they can be accessed, or neglecting to abide by proper data security policies.

Consider Cyber Insurance: Many insurance carriers are now issuing cyber insurance policies that address data and privacy related health care gaps. Losses related to health care information can be substantial. Consult your broker to determine whether such a policy makes sense for your organization.

Taking practical steps to prevent cyber theft in health care raises a variety of legal issues under federal and local laws, and legal counsel should be consulted in advance. Nevertheless, employers that take the initiative with preventative tactics will be in a better position than those that wait for a crisis to occur.

Spencer Hamer, Esq. is a Partner at Michelman & Robinson, LLP and a member of the firm's Labor & Employment Law Department. Feel free to write to him with questions or comments at shamer@mrllp.com. *This article is not be relied upon as legal advice. Consult counsel for advice in specific situations.*

Reprinted with permission from the Washington Healthcare News. To learn more about the Washington Healthcare News visit wahcnews.com.