PUBLICATION

Community Health System's HIPAA Breach: Significant Lessons for Health Care and Non-Health Care Companies

Authors: Alisa L. Chestler
August 20, 2014

On August 18, 2014, Community Health Systems, Inc. (CHS) publicly confirmed, in a filing with the Securities and Exchange Commission (CHS filing), that its computer network was attacked between April and June 2014 by hackers originating from China. Using highly sophisticated malware and technology, the hackers were able to bypass CHS's security and copy and transfer sensitive data, including names and Social Security numbers, for individuals who were referred to or received services from physicians affiliated with CHS in the last five years. According to CHS's filing, the attack and subsequent breach impacted approximately 4.5 million individuals. It was previously believed such hackers were preoccupied with intellectual property; however, the criminals have either branched into new areas or found a new enterprise. CHS's filing noted that CHS conducted an investigation into the breach and is now taking steps to remediate the incident.

This incident sends a clear message that health care companies are just as significant of a target to cyber criminals as are financial and retail institutions. This incident also reinforces the business necessity – for companies across all industries – of having the appropriate protocol in place to prevent, address, and/or mitigate a security incident. If a leading hospital outfit can be breached, all are at risk, and the expense associated with mitigating a breach, separate from any penalties, can be enormous.

Should your company be concerned?

Unfortunately, breaches of personal information – whether by specific attacks, such as those described above, or by accident – have become an increasingly common occurrence. Regulators and legislators, seeing the significant issues resulting from the release of individuals' personal information, have taken legislative action at the federal and state level to specify security controls (such as how personal data must be destroyed or encrypted), to mandate notification and reporting when there is a breach, and to provide for monetary penalties in instances of noncompliance. Here are some issues of which your company should be aware:

Increased Scrutiny: Companies are subject to federal and state laws that provide for heavy fines. And while certain federal laws do not provide for a private right of action, many state laws leave such claims open, and the plaintiffs' bar has been filing lawsuits based on privacy violations with increasing regularity. Furthermore, public companies have been expected, since October 2011, to be prepared to report cyber security incidents to the SEC, and boards of directors have been increasingly anxious about such incidents in recent years.

Audits: Health care companies, whether HIPAA-covered entities or business associates, need to be prepared for the upcoming second round of audits by the Office of Civil Rights, which will commence this fall. A significant number of companies, which will be selected based on geographic and demographic diversity, will be reviewed. Entities that experienced past breaches can also expect some kind of audit from regulators.

Crossing State Lines: The CHS breach highlights a significant area of concern for companies that maintain information for individuals who are located in another state. Most states have implemented laws that overlap federal laws, such as HIPAA, and can be utilized by state attorney generals to pursue actions against companies located outside of the state. Recently, the Attorney General of Massachusetts pursued an action

against a hospital located in Rhode Island. The hospital was fined $150,000 for losing back-up tapes with personal information on Massachusetts residents. It should give everyone great pause to realize the reach across state lines in this instance.

How can your company prevent or be prepared for a breach?

Understand Your Company's Risk Profile: It is crucial to understand the legal landscape in your company's geographic footprint. As many state laws also require notification to state regulators, companies should be prepared to also notify the proper state authorities. It is also important to understand and identify the potential threats to the security of the information in your company's possession.

Implement Appropriate Controls: Implement the appropriate administrative, technical and physical controls based on your company's risk profile.

Assess Your Controls: Your company should frequently audit and assess its measures and controls to ensure that your company is appropriately safeguarding information in its possession.

Read CHS's SEC filing here. If you have questions about performing security risk assessments or other data security issues, please contact a member of Baker Donelson Privacy and Information Security Group.