akrivis LAW GROUP PLLC

Client Alert: February 18, 2015

How Safe is Your Information? How can Companies Protect Themselves in the Wake of Anthem-sized Data Breaches?

Teresa N. Taylor
Partner
202.730.1271
ttaylor@akrivislaw.com
www.akrivislaw.com

In the wake of the recent disclosure of the largest security breach in America at major insurance carrier Anthem, companies are increasingly worried about outside hackers. Yet, data breaches often come from within, and whether intentional or unintentional, companies are liable. The new rule under the Health Insurance Portability and Accountability Act, Health Information Technology for Economical and Clinical Health Act (HIPAA HITECH) expands liability for violations beyond businesses to include employees and third party vendors of the health care entity and substantially increases civil and criminal penalties. What precautions should companies take to protect their clients and employees?

"Software programs and firewalls alone are no longer sufficient to protect a company's secrets or their customers' Personally Identifiable Information (PII) or Personal Health Information (PHI). With cyber-attacks and data theft at an all-time high, companies need to be more vigilant and recognize that most breaches actually arise from within the organization in nearly all situations," says Teresa Taylor, Partner at Akrivis Law Group in Washington, DC. In the past 18 months alone, massive data breaches have occurred at JP Morgan, Home Depot, Target, Sony, and now Anthem, just to name a few. In the case of Sony for instance, news reports state that hackers found a document in the system titled, "Usernames and Passwords" that contained the usernames and passwords of its employees; in the Target breach the systems credentials were stolen from an HVAC contractor and initially used to hack into its corporate system; and in the recent Anthem breach an Administrator's password and other information is suspected to have been used by hackers to gain entry into the company's database.

akrivis LAW GROUP PLLC

How Safe is Your Information? How can Companies Protect Themselves in the Wake of Anthem-sized Data Breaches?

Critical infrastructure industries are more vulnerable than ever, with the health, energy, and financial sectors being the most vulnerable. Even data protection and cyber security technology providers themselves are at risk. Mitigating exposure to liability as a result of data security breaches can save millions per year in lost assets or reputation, intellectual property, customer information, fines, or other damages. Having the most updated technology, a security company, or a firewall is not enough. Companies need to pay as close attention to what is happening inside their companies as they are to potential external threats. Companies need to be diligent in monitoring employee negligence, recklessness, and failure to follow the company's compliance and security protocols.

Corporations very much need to utilize experienced regulatory compliance counsel to evaluate and develop compliance programs. This can include providing training that is catered to different groups of employees and business lines, conducting a risk assessment and gap analysis of security protocols that may currently be in place, working with the technology and security staff and related vendors to ensure efficient implementation of the company's protocols, and creating effective disciplinary measures for those who fail to abide by those protocols. While some deficiencies may be to some extent comprehensible, some are shockingly blatant and overt. Unbelievably, today the most commonly used password remains, "password". This is unacceptable. Simple things like when an employee fails to log off or change a password, or failing to encrypt emails that contain protected health information (which includes simple information such as names, addresses, and emails under HIPAA HITECH) puts the company at risk for both internal and external risks.

Any robust compliance program, especially one that addresses HIPAA HITECH, should also contain provisions that create checks and balances over management and the technology staff as well the company's other employees and vendors that is transparent and provides limited access depending on tasks. Even high-level technology management's (such as CSO's and CTO's) usage and access should be transparent and tempered. High-level technology and compliance management and executives sometimes fail to report breaches and similar risks whether those risks are coming from an internal or external risk because they want to project effective management and control to the board or others. These individuals are themselves often targets because they usually have access to most if not all of the company's security, technology, employee information, and corporate secrets. After a data breach, the CSO or CTO often finds themselves in the position of having to defend their security decisions and method of training or performing quality checks on implementation of compliance protocols. It is therefore prudent that these decisions and processes be transparent and reviewed by the board on a routine basis.

Compliance with HIPAA HITECH could not be any more important than it is now. The new rule went into effect September 2013 and provides steep penalties for violations. Although there is no private cause of action under HIPAA HITECH, it is more troubling that the law provides for the delegation civil and criminal prosecution from the Department of Justice down to the states' Attorneys General, who will not be as versed in the understanding or application of these highly complex federal regulations. Either federal or state prosecutors may opt to prosecute a civil class action on behalf of victims against any violator of the new provisions. The new rule significantly expands liability for violations of HIPAA HITECH. For instance fines range for employees from $500 to $25,000 per violation, and for corporations from $50,000 to $1,500,000 per violation. These fines can stack up quickly where, for example, PHI may

be accessed without authorization multiple times in one day as each time either the same or different PHI is accessed it counts as a separate violation regardless of whether that PHI is accessed in violation of HIPAA HITECH from within the corporation or it is accessed via an external hack into the system.

Under the regulations a breach is defined broadly as an "impermissible use or disclosure" under the Privacy Rule that compromises the security or privacy of the PHI. Such impermissible uses or disclosures are presumed to be in violation of the law until proven otherwise. The notification requirements under the new rule are just as broad in that individual notification of a breach of PHI must be provided "without unreasonable delay, and in no case later than 60 days." (emphasis added). The timeline of "without unreasonable delay" is very open-ended and what may be determined to be reasonable will be fact specific under each breach situation or violation. The new rule, including the notification rule and applicable fines, further extends liability to third party vendors who assist the health care entity in any regard, and this is very wide-sweeping as it includes lawyers, accountants, any subcontractor company, security and software host or monitoring companies, financial processing companies, and so on. Clarity and quality control of compliance protocols should therefore be of grave importance to companies in the health care industry. The reputational loss arising from a public notice of a breach often significantly impacts a company's bottom line absent any civil or criminal fines for compliance violations. HIPAA HITECH is a dense, complex law, and it is just as important that a corporation be prudent and preemptive by implementing plan to follow should a breach or suspected breach occur and that it utilize regulatory counsel to assist in determining whether notification actually need take place. On the flip side, companies often rush to send out notification of a breach in effort to be in compliance with the law when a proper legal analysis of the situation may actually reveal that the facts do not constitute a breach requiring notification.

The Health and Human Services, Office of Civil Rights is tasked with enforcement of HIPAA HITECH. On their website is what has been termed the "wall of shame". The wall of shame presently lists 1132 companies who have violated these provisions and been fined and runs the gamut from small pediatric offices and solo practitioners to large corporations that have are routinely fined in ranges from $50,000 to several millions. The violations run from simple and careless actions, such as where an employee took an unencrypted thumb drive from work and it was thereafter stolen from his car (company received a fine of $150,000), to massive data breaches such as what we have just witnessed with Anthem. Anthem reports that none of the information accessed or disclosed during the breach is protected health information (PHI) because there were no health records involved. This is an incorrect legal application. The definition of PHI in HIPAA HITECH includes otherwise benign information such as names, addresses, and emails. This is the very type of information that was illegally accessed in Anthem's breach according to news sources. Health and Human Services has publically commented that it considers the information accessed during the Anthem breach to be within the legal definition of PHI provided by HIPAA HITECH. Hopefully we will not see a breach this size again anytime soon.

For more information on HIPAA HITECH compliance please contact Teresa N. Taylor, Partner at Akrivis Law Group, PLLC, at (202) 730-1271, or ttaylor@akrivislaw.com.