Health Care Law

The HIPAA Security Rule: Your Best Defense Against Cybersecurity Liabilities

It seems that every day there is another story of a cyberattack in the news. Big-name companies targeted by hackers in order to steal confidential information or disrupt service include Home Depot, Target, JPMorgan Chase, and Sony. Besides the economic and reputational fallout that occurs with each data breach, companies are now facing shareholder derivative actions, class actions and significant regulatory liability from federal and state agencies that have exponentially ramped up their enforcement efforts concerning data breaches.

John J. Cooney

Data breaches and the related risks and liabilities are nothing new for entities regulated by the Health Insurance Portability and Accountability Act (HIPAA). There are numerous regulations and affirmative responsibilities associated with safeguarding protected health information (PHI) and electronic protected health information (EPHI), and reporting of data breaches. Noncompliance and with HIPAA can lead to a range of U.S. Department of Health & Human Services, Office for Civil Rights (OCR) enforcement and penalties.

In other words, a HIPAA-regulated entity is already accountable for the protection of its industry data. One could assume that it should not have to worry about complying with other federal and state regulations concerning data security and reporting of data breaches. That would be a wrong assumption.

State and Federal Liability for Privacy Breaches

For instance, the Federal Trade Commission (FTC) has taken the position that its broad powers to regulate unfair and deceptive practices, under Section 5 of the FTC Act, 15 U.S.C. § 45, include jurisdiction of the security and privacy practices of HIPAA-regulated entities.[1] Indeed, the FTC appears to be the anointed agency when it comes to enforcing privacy across all industries.

For example, on January 12, 2015, President Obama made the first presidential visit to the agency since 1937 to announce that consumer privacy initiatives would be one of his top priorities in 2015.[2] Moreover, in March, the FTC provided Congressional testimony on proposed data security legislation that would provide a federal standard for data security and reporting of breaches.[3] Notably, the proposed legislation provides the FTC with enforcement authority along with state attorney generals over violations of data security requirements or consumer notification provisions.[4]

In sum, the writing is on the wall. HIPAA-regulated entities are subject to investigations and enforcement actions for privacy and security breaches by both the OCR and the FTC.

Moreover, a HIPAA-regulated entity must also comply with the New York State Information Security Breach and Notification Act (NYS Act).[5] HIPAA regulates the safeguarding and reporting of data breaches concerning PHI and EPHI, while the NYS Act provides New York residents with the right to be notified when a data breach has resulted in the exposure of their personal information in combination with other data defined as private information, such as a social security number, driver's license number, or credit or debit card number.[6]

Under the NYS Act, a business is required to notify residents "in the most expedient time possible and without unreasonable delay" by either written notice, electronic notice, or telephone notification.[7] Moreover, notice must include a description of the categories of information that were, or are believed to have been, acquired. The New York Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination must also be notified.[8]

Finally, following President Obama's announcement earlier this year, Attorney General Eric T. Schneiderman formally announced that he will propose legislation to significantly expand the definition of private information, and to impose affirmative obligations on entities to safeguard such private information through appropriate technical, administrative and physical safeguards and to notify residents in the event of a cyberattack or data breach.[9] In other words, whether under the current NYS Act, or a significantly enhanced NYS data privacy law, a HIPAA-regulated entity must safeguard more than just health information.

HIPAA Standards for Protecting Privacy

Luckily for HIPAA-regulated entities, there is already a set of national standards that, if complied with, will provide a roadmap to safeguard private information to comply with HIPAA, as well as to mitigate regulatory liability under current or proposed federal and state laws. The HIPAA Security Rule (Security Rule) contains a set of security standards divided into the same categories as Attorney General Schneiderman announced earlier this year: technical, administrative, and physical safeguards.[10]

As an initial step, the Security Rule requires that entities conduct a risk assessment of their organizations to identify vulnerabilities and implement the aforementioned technical, administrative and physical safeguards.

Examples of technical safeguards within the Security Rule are encrypting EPHI being stored and/or transmitted, maintaining audit logs to record activity, and enforcing authentication controls to verify that an employee is authorized to access the EPHI.[11] Administrative safeguards include policies and procedures, assignment of data security responsibility, and employee training.[12] With regard to physical safeguards, an entity must have measures to account for transfer, removal, disposal, and re-use of EPHI. They must also have protocols to restrict physical access to workstations, laptops and devices, and to recover off-site computer backups.[13]

It is highly recommended that the organization retain a team, consisting of counsel and their trusted information technology partners, to conduct a risk assessment and ensure proper identification and implementation of the aforementioned safeguards and cybersecurity best practices across industries, such as a written information security program (WISP). The findings of the risk assessment would be shielded by the attorney-client privilege.

Moreover, even the "addressable" HIPAA security standards, which are provided to give an entity some flexibility for implementation, should be treated as "required" because it is likely that the "addressable" security standards will become required under either new state or federal regulations. In other words, given the proposed federal and state initiatives and increased enforcement actions, a HIPAA-regulated entity will spend more time and money documenting a legitimate reason for not implementing the safeguard, rather than putting the necessary protection in place.

Conclusion

Given the long-standing and proven HIPAA standards, state and federal agencies are now adopting some of the same standards. Thus, a HIPAA-regulated entity should comply with the Security Rule in full and for all data rather than just PHI or EPHI. However, if a HIPAA-regulated entity has not yet complied with the Security Rule, it is far from alone. According to recent estimates, two-thirds of HIPAA-regulated entities have not completed an accurate risk assessment and, thus, are failing to safeguard the data. In other words, it is not too late to protect your organization.

John J. Cooney, Esq. serves Of Counsel to Ruskin Moscou Faltischek where he is chair of the Firm's Cybersecurity and Data Privacy practice group. He is also a member of the Firm's Health Law Department and the White Collar Crime and Investigations practice group. Prior to becoming an attorney, Mr. Cooney was trained as a software engineer and had over a decade of experience analyzing and developing technology solutions for Fortune 500 companies. He can be reached via e-mail at jcooney@rmfpc.com.

1 *See In re LabMD, Inc.*, FTC, No. 9357, *dismissal denied* (Jan. 16, 2014).
2 President Barack Obama, *Remarks at the Federal Trade Commission* (Jan. 12, 2015), at https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.
3 *Prepared Statement of the Federal Trade Commission on Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015, Before the Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, United States House of Representatives*, 113th Cong. (2014).
4 H.R. 1770, 114th Cong. (2015).
5 New York Information Security Breach and Notification Act, *codified as amended at* Gen. Bus. L. § 899-aa, and State Tech. L. § 208.
6 Gen. Bus. L. § 899-aa.
7 *Id.*
8 *Id.* (if more than 5,000 New York residents are affected, various consumer reporting agencies must also be notified).
9 *A.G. Schneiderman Proposes Bill To Strengthen Data Security Laws, Protect Consumers From Growing Threat Of Data Breaches*, Jan. 15, 2015, http://www.ag.ny.gov/press-release/ag-schneiderman-proposes-bill-strengthen-data-security-laws-protect-consumers-growing.
10 45 CFR § 164.304.
11 45 CFR § 164.312.
12 45 CFR § 164.308.
13 45 CFR § 164.310.