Bloomberg Law®

Privacy and Security Law Report®

NY Cybersecurity Reg

New York's new cybersecurity regulation will regulate the data security practices of health-care insurers with a set of rules that are the most comprehensive in the U.S. These rules will require many health-care insurers to take a fresh and comprehensive look at their cybersecurity programs, governance and defenses to meet the deadlines, the author writes.

Dueling Cybersecurity Regulations for Health Care: HHS Meets New York State

BY CRAIG A. NEWMAN

Data security regulation for health-care insurers that operate in New York just got more complicated. For years, the U.S. Department of Health and Human Services' Office for Civil Rights—the industry's primary data security regulator—has zealously policed the health care field. In fact, so far in 2017, the agency has already brought four data security enforcement actions. The most recent was the February 2017 $5.5 million settlement with Memorial Healthcare System—matching the largest civil monetary fine ever imposed against a single organization—because of weak internal controls that permitted employees to improperly access more than 100,000 patient records.

And now New York has gotten into the act with a completely different set of rules that are the most comprehensive of any U.S. state. Earlier this month, New York's top banking and insurance regulator threw down the proverbial gauntlet—or, perhaps more of a sledgehammer— with its new cybersecurity regulation which has broad implications for health-care insurers that operate in New York. The regulation will force health-care insurers to navigate a minefield of new and far more exacting technical, legal and governance requirements than the industry specific regulations already in place including those under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). The New York rules just took effect on March 1 and will phase in over two years but many detailed requirements must be put in place within the first 180 days.

This will require many health-care insurers to take a fresh and comprehensive look at their cybersecurity programs, governance and defenses to meet the deadlines. The regulation also places additional demands on an insurer's third-party vendors—now indirectly covered by the new rules—including health care providers and outside consulting, accounting and law firms, among others.

Craig A. Newman is a partner at Patterson Belknap Webb & Tyler LLP in New York and chairs the firm's Privacy and Data Security Practice.

Background: The New York Regulation

On March 1, the New York State Department of Financial Services (DFS) issued a ''first in the nation'' cybersecurity regulation designed to protect financial institutions and insurance companies, their information technology systems, and their customers from cybercrime. The regulation applies to any entity operating with a ''license'' or ''similar authorization'' under New York's ''Banking Law, the Insurance Law or the Finan-

 ISSN 1538-3423

cial Services Law''—including foreign and out-of-state affiliates of DFS-regulated entities. It directly covers health-care insurers that operate in the state.

Health-care insurers are accustomed to regulation. The HIPAA Security Rule already requires that they maintain data security programs that are reasonable in view of their scale, complexity and resources but does not dictate particular measures that must be undertaken. The New York regulation takes a starkly different approach with its matrix of specific risk-based governance, process and technical requirements. Although the new regulation includes a degree of flexibility to fit each institution's risk profile, it has 23 different sections and is far more detailed and accountability-oriented than other data security regimes. And in a clear departure from existing data security regulatory norms, the new DFS regulation holds an institution's senior leadership responsible for compliance by requiring the filing of an annual compliance certificate attesting to an institution's adherence to the regulation.

The New York regulation requires, in general, that DFS-regulated health-care insurers have state-approved plans in place to protect their businesses, information systems and the personal information of their customers. The rules require that each health-care insurer start by conducting a ''risk assessment'' to drive the scope of the organization's overall cybersecurity program. The cybersecurity program must be ''designed to ensure the confidentiality, integrity and availability'' of its information systems. Notably, the cybersecurity program is not necessarily a written, standalone document but rather the underlying system, process and procedures by which a covered entity ensures its compliance with the DFS regulation.

At a minimum, the cybersecurity program must do six things: (1) identify internal and external cybersecurity risks; (2) use defensive infrastructure and the implementation of policies and procedures to protect information systems and non-public information; (3) detect cybersecurity events; (4) respond to, detect and mitigate the effects of cybersecurity events; (5) recover from cybersecurity events; and (6) fulfill regulatory reporting requirements.

Beyond the cybersecurity program, there is a laundry list of additional requirements ranging from the development and implementation of a 14-point cybersecurity policy to employee training, board and senior leadership engagement to highly technical requirements like encryption, access controls and different types of internal monitoring or vulnerability assessments.

In a clear departure from existing data security regulatory norms, the new regulation holds an institution's senior leadership responsible for compliance

For DFS-regulated health-care insurers, the new rules present a regulatory scheme—and regulatory expectations—that impose new obligations and new approaches to data security. Here is a brief look at several of these important new requirements:

Accountability: Cyber Czar and Corporate Leadership

Unlike existing health-care data security regulation, the New York rules are based on a foundation of corporate accountability. In the first instance, the New York regulation requires the designation of a ''qualified individual'' to serve as a chief information security officer (CISO). The CISO is responsible for overseeing, implementing and enforcing the covered entity's cybersecurity program and policy. Covered entities have the option of engaging a third-party service provider to serve as the CISO, but retain responsibility for compliance with the CISO requirements and must appoint a senior employee to oversee the third-party service provider.

Not surprisingly, the CISO's responsibilities are substantial including delivering a bi-annual report to the board or equivalent governing body that covers, ''to the extent applicable,'' the following:

- an assessment of the confidentiality, integrity and availability of the covered entity's information systems;
- exceptions to the covered entity's cybersecurity policies and procedures;
- identification of cybersecurity risks;
- an assessment of the cybersecurity program's effectiveness;
- proposed steps to remedy inadequacies in the cybersecurity program; and
- a summary of material cybersecurity events.

Beyond the CISO's role, the DFS regulation requires engagement and accountability at the top of an organization. According to the regulation, senior management ''must take'' cybersecurity issues ''seriously and be responsible for an organization's cybersecurity program.'' That responsibility starts with review of the organization's cybersecurity policy. The regulation requires that the board of directors, an ''appropriate committee of the board of directors, or a ''senior officer'' approve the policy. The chairperson of the board of directors or a senior officer must also certify in writing to DFS annually that the organization's cybersecurity program complies with the regulation.

New York Regulation Far Broader Than HIPAA

And, the New York regulation covers far more sensitive information than under HIPAA. The HIPAA Privacy Rule covers individually identifiable health information—called protected health information (PHI), and is subject to certain general data security safeguards. The HIPAA Security Rule protects a subset of that information—individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form (called e-PHI). By contrast, the New York regulation protects three different categories of sensitive information—only the last category of which directly overlaps with PHI or e-PHI:

- business related information, the tampering with which or unauthorized disclosure of which would cause a material adverse impact to the business;
- information about an individual which because of name, number, personal mark or other identifier can be

  PVLR ISSN 1538-3423

used to identify such individual, in combination with any one or more of the following data elements: social security number; drivers' license number or identification; account number (credit or debit); any security code, access code or password that would permit access to a financial account; or biometric records; and

■ information about the mental, physical, or behavioral health of an individual or the individual's family or household.

The New York rules also apply to the security of ''information systems'' generally. This means that DFS-regulated health-care insurers will need to broaden their approach to cybersecurity protection to include these new elements not already covered by existing federal health-care regulation.

Substantial Obligations on Third-Party Vendors

The new regulation not only contains extensive requirements for covered entities, but also requires third-party vendors with access to a DFS-regulated organization's information technology network or non-public information to meet minimum cybersecurity standards. Under HIPAA, covered health-care entities must bind third parties that will receive protected health-care information to comply with HIPAA's requirements in a ''Business Associate Agreement.'' Such agreements may identify specific data security protocols that must be followed, but technical requirements are not mandated.

By contrast, the New York regulation sets out data security rules and protocols that regulated institutions must impose on their vendors and business partners. The regulation's focus on third-parties connected to covered entities is likely DFS's response to the massive data breaches that have grabbed headlines over the past few years—in addition to numerous related class action lawsuits and derivative demands—involving cybersecurity vulnerabilities of vendors with access to company networks.

The reporting requirements under the New York regulation are also far stricter than under the Health Insurance Portability and Accountability Act.

Under the New York regulation, covered entities are required to develop and implement written policies and procedures to ensure the security of any IT systems or non-public information that can be accessed by their vendors. At a minimum, these policies must identify the risks arising from third-party access, impose cybersecurity standards on the third-party vendors, and create a due-diligence process for evaluating vendors. Moreover, organizations must establish ''relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers.'' To ''the extent applicable,'' those guidelines must address:

■ use of multi-factor authentication to limit access to sensitive IT systems or non-public information;

■ use of encryption of all non-public information—both ''in transit and at rest'';

■ notice from the third-party provider to the regulated entity in the event of a breach or potential cybersecurity-related event;

■ representations and warranties from the third-party provider that the system or product provided ''is free of viruses, trap doors and other mechanisms that would impair the security'' of the organization covered by the regulation; and

■ representations and warranties from the third-party provider addressing its cybersecurity and policies that relate to the security of the covered entity's information systems and non-public information.

Regulatory Notice Provisions Far Different

The reporting requirements under the New York regulation are also far stricter than under HIPAA. Unique among state and federal breach reporting laws, the new DFS regulation imposes a mandatory notification process for any ''material'' cybersecurity event, as defined by the regulation. Within 72 hours ''from a determination'' that such a cybersecurity event occurred, a covered entity must inform the DFS of the event. A cybersecurity event is ''material'' if it falls in the following categories:

■ a cybersecurity event for which notice is required to any *other* government or self-regulatory agency; *or*

■ a cybersecurity even that has a ''reasonable likelihood of materially harming any material part of the normal operation(s)'' of the Covered Entity.

Under HIPAA's Breach Notification Rule, institutions must report the breach of unsecured health information to the HHS without reasonable delay but in no event later than 60-days after discovery of the breach, or, if affecting fewer than 500 individuals, within 60 days of the end of the calendar year in which the breach occurred.

Conclusion

The New York regulation isn't likely to be the last word on data security for the industry. The National Association of Insurance Commissioners is considering a model law that each state could adopt—outlining how insurers must safeguard consumer information and respond in the event of a data security incident. The model law was unveiled last year but has undergone revisions in response to criticisms raised by the industry and consumer groups.

For health-care insurers already subject to extensive federal data security regulation, the New York cyber regulation imposes additional—and sweeping—burdens and requirements. No other data security regulation has demanded this combination of accountability, senior leadership engagement and across-the-board detail. And there's no doubt that DFS will hold those institutions accountable for ball drops.