

Bloomberg
Law®

Patterson Belknap

New York's Cybersecurity Regulations for Financial Institutions & Health Care



New York's Cybersecurity Regulation for Financial Institutions

A New Age of Cybersecurity Regulation: Raising the Bar and Demanding Leadership Accountability

Authors:

Craig A. Newman

Alejandro Cruz

Kade Olsen

Simone Silva-Arrindell

Leigh Barnwell

Patterson Belknap Webb & Tyler LLP

About the Publication:

This mini-treatise, *New York's Cybersecurity Regulation for Financial Institutions, A New Age of Cybersecurity Regulation: Raising the Bar and Demanding Leadership Accountability*, authored by Patterson Belknap Webb & Tyler LLP, and published by and available on **Bloomberg Law** provides a general overview of the sweeping new cybersecurity regulation issued by the New York State Department of Financial Services, the state's top banking and insurance regulator, focusing on its core rules and requirements. This publication also provides practical guidance regarding issues that affected institutions might want to consider as they implement the requirements of the regulation.

About Patterson Belknap's Privacy and Data Security Practice:

The Patterson Belknap Privacy and Data Security practice provides public and private organizations—including financial services firms, asset managers and funds, retailers, hospitality, media and technology companies, manufacturers, insurance companies, tax-exempt organizations, and law firms—with comprehensive services in this vital area. The firm's attorneys combine decades of experience spanning from the public and private sectors, including experienced litigators, corporate advisors and former federal prosecutors with deep experience in all aspects of privacy and data security. The group advises on a broad range of issues including prevention and compliance, risk mitigation, data breach response, special board and committee representation, internal investigations, and litigation. Patterson Belknap also draws on valuable resources, including highly experienced forensic consultants, security professionals, and crisis communications teams, who add insight and value on key aspects of cybersecurity matters.

About the Firm:

Patterson Belknap Webb & Tyler LLP is a New York City based law firm with over 200 lawyers. The firm is on *The American Lawyer's* 2016 "A-List" of the 20 leading law firms in the United States. Patterson Belknap delivers a full range of services across approximately 20 practice groups in both litigation and commercial law. For more information, please visit www.pbwt.com.

About Craig Newman:

Craig A. Newman is a recognized leader in both complex financial litigation and global cybersecurity. With more than twenty years as a litigation partner and General Counsel at both a multi-billion dollar international private equity firm and F500-owned media consortium, Craig represents Fortune 500 companies, their boards and leadership teams. In his cybersecurity work, Craig represents clients in litigation, regulatory and governance matters, and the management of risks associated with data security practices and policies including data breach preparedness and response. He chairs Patterson Belknap's Privacy and Data Security Practice and is a founding contributor to the firm's blog, www.DataSecurityLaw.com. Craig also sits on the Bloomberg Law Innovation Advisory Board. A former journalist, Craig appears regularly on national television including CNBC, CNN and Bloomberg, discussing issues at the intersection of business, law, cybersecurity and data privacy, and has written for *The New York Times*, *The Washington Post*, *The Wall Street Journal* and *Financial Times*. He was named as one of the *National Law Journal's* 2015 "Cybersecurity & Data Privacy Trailblazers."

About Bloomberg Law:

Bloomberg Law helps legal professionals provide world-class counsel with access to actionable legal intelligence in a business context. Bloomberg Law delivers a unique combination of practical guidance, comprehensive primary and secondary source material, trusted content from Bloomberg BNA, news, time-saving practice tools, market data and business intelligence. For more information, visit www.bna.com/bloomberglaw.

Bloomberg Law: Privacy & Data Security brings you streamlined access to the expertise of Bloomberg BNA's privacy and data security editorial team, contributing practitioners, and in-country experts together with unmatched practice tools to help you quickly respond with confidence to client inquiries.

In Practice tools include exemplar policies and provisions, checklists, and forms to facilitate your drafting needs for privacy and data security tasks such as:

- New York Cybersecurity Regulation for Financial Institutions Managing a Data Breach
- Managing Privacy and Data Security Risk in Mergers
- Designing a Privacy Policy
- Cross-Border Data Transfer

Introduction

Cybersecurity is one of the most critical challenges facing our nation and our economy. U.S. regulators on both the state and federal level are working to keep pace with the challenges and risks posed by cybercrime.

On March 1, 2017, a sweeping new cybersecurity regulation was issued by the New York State Department of Financial Services, the state's top banking and insurance regulator. The regulation affects more than 3,000 institutions that operate in the state as well as many of their key third-party vendors. The regulation - in some respects - is unprecedented in its detail and focus on leadership accountability.

Patterson Belknap Webb & Tyler LLP is pleased to release "A New Age of Cybersecurity Regulation: Raising the Bar and Demanding Accountability." Our publication provides a general overview of this new regulation, focusing on its core rules and requirements. We also raise issues that affected institutions might want to consider as they implement the requirements of the regulation.

Craig A. Newman
Partner & Chair, Data Security & Privacy
Practice Patterson Belknap Webb &
Tyler LLP
New York, New York

A new age of cybersecurity regulation: Raising the bar and demanding accountability

By Craig A. Newman, Alejandro Cruz, Kade Olsen, Simone Silva-Arrindell, and Leigh Barnwell Patterson Belknap Webb & Tyler LLP, New York*

I. Regulatory Overview

A. Introduction

On March 1, 2017, the New York State Department of Financial Services (DFS) issued a new cybersecurity regulation designed to protect financial institutions, their information technology systems, and their customers from cybercrime¹. This “first-in-the-nation regulation” requires many of the more than 3,000 financial institutions, insurance companies, health plans, charitable institutions, and other organizations regulated by DFS to take a fresh and comprehensive look at their cybersecurity preparedness, governance, internal controls, and defenses. It applies directly to any entity operating with a “license … or similar authorization under [New York’s] Banking Law, the Insurance Law or the Financial Services Law”², –including many foreign and out-of-state branches of DFS-regulated entities.

The regulation provides a basic framework within which organizations are required to develop a comprehensive cybersecurity program best suited to address their specific risk profile. Although the new regulation includes a degree of flexibility and bears some similarities to guidelines and regulations issued by other regulatory bodies, it has 23 different sections and is far more detailed and accountability oriented than most other comparable data security regimes. Significantly, in a clear departure from existing data security regulatory standards, the new DFS regulation holds an institution’s senior leadership accountable by requiring an annual compliance certificate signed by a senior officer or board member.

Given the DFS’s broad authority and history as an aggressive regulator, the risks of noncompliance with the new regulation are substantial. And prompt implementation is

* Craig A. Newman, a partner in the New York office of Patterson Belknap Webb & Tyler LLP, chairs the firm’s Privacy and Data Security Practice. He may be reached at cnewman@pbwt.com. Alejandro Cruz, Kade Olsen, Simone Silva-Arrindell, and Leigh Barnwell are all associates at the firm.

The information presented here is for general informational purposes only and should not be construed as specific legal advice. The information is also summary in nature. Please refer to the New York Department of Financial Services “Cybersecurity Requirements for Financial Services Companies” for a full statement of the regulation and applicable requirements.

¹ Cybersecurity Requirements for Financial Services Companies,

² 23 NYCRR 500.01(c).

required. As the regulation states, “[i]t is critical for all regulated institutions … to move swiftly and urgently to adopt a cybersecurity program.” 23 NYCRR 500.00. Notwithstanding the mandate to act quickly, the complexity of the new regulation means that affected organizations will need to proceed methodically to ensure compliance with the regulation, and should consider appropriately documenting their decision-making process at key junctures.

II. Accountability

A. Corporate Governance

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.” 23 NYCRR 500.00.

That responsibility starts with the organization’s “Cybersecurity Policy.” According to the new regulation, each covered entity must implement and maintain a written policy laying out its policies and procedures for the protection of its information systems and any nonpublic information³ stored on those systems. 23 NYCRR 500.03. The policy must address, at a minimum, data governance, access controls, disaster recovery planning, performance planning, network security, consumer data privacy, third-party management, and incident response. We discuss each of these topics below.

Critically, the policy must be approved by the organization’s board or a senior officer. The regulation requires that the board of directors, an “appropriate committee thereof,” or a “Senior Officer” approve the policy. 23 NYCRR 500.03. An organization must also certify in writing annually to the DFS that its cybersecurity program complies with the regulation. 23 NYCRR 500.17.

³The regulation expressly defines nonpublic information. 23 NYCRR 500.01(g). First, such information includes any business-related information that, if tampered with or disclosed, would cause a material adverse impact to the business. Second, it includes any information that can be used to identify an individual, “in combination with any one or more of the following elements”: (i) social security number; (ii) driver’s license or similar number; (iii) account or credit card number; (iv) security code or password that would permit access to an individual’s financial account; or (v) biometric records. Finally, it includes any information (except for age or gender) created or derived by a health care provider related to: (i) any mental condition; (ii) the provision of any health care; and (iii) the payment for health care.

Patterson Belknap Commentary

No prior state or federal regulations have come close to requiring this level of accountability from an organization's directors or senior management. Accountability of this nature also raises the prospect of potential liability at the top of an organization. Covered entities will need to promptly develop procedures for educating and updating senior management and/or board members regarding their responsibilities under the new regulation.

Covered entities should also consider reviewing relevant insurance policies, including directors and officers (D&O) coverage, to account for the new layer of potential liability imposed by the DFS regulation.

B. Chief Information Security Officer (CISO) Designation

Covered entities must designate a "qualified individual" to serve as a Chief Information Security Officer (CISO). 23 NYCRR 500.04. The CISO is responsible for *overseeing, implementing, and enforcing* the covered entity's cybersecurity program and policy. Covered entities may employ a third-party service provider to serve as the CISO, but each covered entity electing to do so must:

- retain responsibility for compliance with the CISO requirements;
- designate a senior member of its personnel to oversee the third-party service provider; and
- require the third-party service provider to maintain a cybersecurity program that meets the DFS's regulations.

The CISO's responsibilities are substantial and require communication with senior management and the board of directors (or a subcommittee of the board). Highlighting, once again, the regulation's focus on senior-level involvement, the CISO must deliver a report at least annually to the board of directors or equivalent governing body. 23 NYCRR 500.04(b).

The board report, "to the extent applicable," must include 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 cyber 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.

In addition to reporting internally, the CISO must report to the DFS Superintendent upon request. 23 NYCRR 500.02(d).

Given the CISO's significant and overall responsibilities for cybersecurity, some smaller covered entities—depending on the circumstances—may wish to consider retaining an experienced and qualified third-party service provider to serve as the CISO.

Patterson Belknap Commentary

Given the scope of the CISO's responsibilities under the regulation, covered entities should consider a comprehensive policy governing the CISO's role within an organization. Such a policy should be reviewed and updated as needed, based on DFS commentary, enforcement expectations, and other pertinent developments.

Organizations have latitude in designating a CISO from within or outside of the organization, as covered entities may use the services of a third party to fill this role. Both options may present potential challenges, and a careful assessment of the risks and benefits of each option should be done before deciding the course of action best suited to the organization's resources and risk profile.

III. Implementation

A. Risk Assessment, Cybersecurity Program, and Cybersecurity Policy

Three overarching requirements of the regulation will drive its implementation: the Risk Assessment, the Cybersecurity Program, and the Cybersecurity Policy.

The regulation requires covered entities to develop a Cybersecurity Program (23 NYCRR 500.02) and Cybersecurity Policy (23 NYCRR 500.03) that comply with DFS requirements. According to the regulation, the central factor in developing both the Cybersecurity Program and Cybersecurity Policy is the Risk Assessment (23 NYCRR 500.09). The Risk Assessment must consider the “particular risks” to a company’s business “sufficient to inform the design of the cybersecurity program required.” 23 NYCRR 500.09(a). Risk Assessments must be performed periodically and “updated as reasonably necessary … to respond to technological developments and evolving threats.” *Id.* From a compliance standpoint, the outcome of these periodic Risk Assessments may serve to refine some covered entities’ obligations under the regulation (especially as firms become more cyber-mature), as many requirements apply only to “the extent applicable” based on the Risk Assessment. See, e.g., 23 NYCRR 500.06(a), 500.11(a).

Risk Assessments, which must be carried out "in accordance with written policies and procedures," 23 NYCRR 500.09(b), shall be documented and must include the following: (1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the organization; (2) criteria for the assessment of "confidentiality, integrity, security and availability" of the organization's information systems and nonpublic information (as defined in the regulation), including existing controls in the context of identified risks; (3) requirements describing how identified risks are either mitigated or accepted and how the organization's Cybersecurity Program will address those risks. Id.

Every covered entity must then develop a Cybersecurity Program that addresses each of the applicable DFS requirements. The Cybersecurity Program "shall be based on the Covered Entity's Risk Assessment" and must be "designed to ensure the confidentiality, integrity and availability" of its information systems. 23 NYCRR 500.02. Notably, the Cybersecurity Program is not necessarily a written, stand-alone document. Rather, it consists of 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 cyber risks; (2) use defensive infrastructure and the implementation of policies and procedures to protect information systems and nonpublic 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. 23 NYCRR 500.02(b).

Finally, as discussed above, a covered entity must create a Cybersecurity Policy. 23 NYCRR 500.03. The Cybersecurity Policy must also be based on the organization's Risk Assessment and should address the following fourteen specific areas (some of which overlap with the regulation's stand-alone requirements) to "the extent applicable":

- information security;
- data governance and classification;
- asset inventory and device management;
- access controls and identity management;
- business continuity and disaster recovery planning and resources;
- systems operations and availability concerns;
- systems and network security;
- systems and network monitoring;
- systems and application development and quality assurance;

- physical security and environmental controls;
- customer data privacy;
- vendor and third party service provider;
- risk assessment; and
- incident response.

B. Day-To-Day Requirements

The regulation also contains a series of detailed day-to-day requirements—ranging from access controls to employee training—that covered institutions must integrate into their overall Cybersecurity Policy, “to the extent applicable” to their operations.

1. Data Governance and Classification

Generally speaking, data classification and data mapping are considered initial steps in developing a Cybersecurity Policy. Organizations must identify how they collect, store, and transmit sensitive data and nonpublic information. While this can be a resource-intensive process, it will likely pay dividends over time. The Cybersecurity Policy should therefore articulate a process for identifying and categorizing different types of sensitive information within an organization.

While covered entities may identify additional categories of sensitive information to be protected, the DFS regulation identifies three categories of nonpublic information that must be protected (23 NYCRR 500.01(g)):

- 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 that—because of name, number, personal mark, or other identifier—can be used to identify such individual, in combination with any one or more of the following data elements: social security number; driver’s 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.

In addition to data classification, covered entities are required to establish a data governance policy. 23 NYCRR 500.03(b). The regulation, however, does not provide guidance as to the specific requirements of such a policy.

Patterson Belknap Commentary

Covered entities may want to consider in appropriate instances utilizing “data stewards” who have expertise on specific categories of sensitive data.

When sensitive information is collected, shared, and accessed across different business units of a covered entity, the Cybersecurity Policy should coordinate security activities and controls between and among the relevant departments.

Covered entities are required to protect sensitive information at all stages of its life within the organization: its creation or collection, its day-to-day use and storage, its transmission inside and outside the organization, and ultimately its deletion, destruction, and disposal.

2. Access Controls and Identity Management

Access controls and identity management go hand in hand with data governance and information security. As part of their Cybersecurity Policy, covered entities should create a framework for managing the electronic identities of those who have access to the organization’s information systems and their corresponding access privileges for various categories of data. The regulation specifically requires companies to “limit user access privileges” to systems that “provide access to Nonpublic Information,” and those privileges must be reviewed and modified on a regular basis. 23 NYCRR 500.07.

Patterson Belknap Commentary

Developing access controls is ancillary to other DFS requirements—including requirements governing network and physical security, vendor data security, and multi-factor authentication.

Each covered entity must “periodically review” the access privileges of its employees. At a minimum, companies should consider reviewing an employee’s access privileges when he or she changes positions, but covered entities should consider going further depending on the circumstances. For example, periodic reviews and reconciliations could provide opportunities to clean-up and refine access privileges based on routine changes in personnel and company structure.

3. Systems and Network Security

As part of the Cybersecurity Program, covered entities should create policies regarding the security of their internal networks. 23 NYCRR 500.03(g). In particular, companies should consider how their electronic systems connect with third parties or other external entities and develop policies for managing the security of those external network connections. This will be especially important for covered entities with network connections to third-party vendors and contractors, which we discuss below.

The Cybersecurity Policy should also incorporate procedures for regular internal systems and network monitoring, as appropriate, to assess the capacity and performance of the systems and network, as well as compliance with security protocols. 23 NYCRR 500.03(h).

4. Physical Security and Environmental Controls

The Cybersecurity Policy must address physical security for the information systems infrastructure. Covered entities must also specify environmental controls that will ensure the integrity and continued availability of the data in the event of man-made or natural disasters or other potential disruptions. 23 NYCRR 500.03(j).

Patterson Belknap Commentary

Organizations should consider developing a comprehensive protocol for controlling access to their most critical information systems considering, among other factors, the firm's overall risk profile, its physical storage of (and use of safeguards for) sensitive information, and its access limitations for relevant personnel.

This is another area where an organization might benefit from a periodic and documented review to ensure that access controls remain current.

5. Systems Operations and Availability

The Cybersecurity Policy must also address the availability of information systems. Covered entities should ensure that necessary systems are available as needed to employees and customers by adopting policies regarding hardware maintenance and repairs, operating system functionality, software upgrades, and adequate bandwidth, among other topics. 23 NYCRR 500.03(f).

Patterson Belknap Commentary

Network capacity, performance, and availability constraints are clearly of concern to DFS. Covered institutions would be well advised to engage in a periodic review of these issues to ensure compliance with the regulation.

6. Systems and Application Development and Quality Assurance

Entities must ensure that their information systems, applications, and security programs work as designed and developed to address vulnerabilities. 23 NYCRR 500.03(i). To that end, covered entities must prepare “written procedures, guidelines and standards” to ensure “secure development practices” for in-house applications and systems and “procedures for evaluating, assessing or testing” externally developed applications and systems. 23 NYCRR 500.08(a).

Patterson Belknap Commentary

The procedures, guidelines, and standards for system and application security must be assessed and updated by the CISO “as necessary.” 23 NYCRR 500.08(b). Given the “as necessary” language, organizations should consider reviewing the security of their applications and systems on a routine basis, subject to their particular risk profile and other relevant circumstances.

7. Data Retention, Destruction, and Audit Trails

The regulation sets forth specific guidelines for the retention and destruction of data. At a minimum, a covered entity must implement, “to the extent applicable and based on its Risk Assessment,” an audit trail system that tracks and maintains data “to reconstruct material financial transactions sufficient to support normal operations and obligations,” as well as to detect and respond to cybersecurity events. 23 NYCRR 500.06. Audit trail records must be retained for at least five years. *Id.*

There are, however, limits on the data retention required by the regulation. Covered entities must implement policies and procedures for the timely destruction of nonpublic data that is “no longer necessary for business operations or for other legitimate business purposes of the Covered Entity.” 23 NYCRR 500.13. Covered entities may retain data or information when it is otherwise required by law or regulation “or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.” *Id.*

Patterson Belknap Commentary

The audit-trail requirement is significant. Organizations must maintain audit trails that allow for the reconstruction of financial transactions sufficient to support normal operations, and designed to detect and respond to cybersecurity events.

Covered entities and their counsel may wish to consider, as necessary, obligations to discard data in light of existing document retention policies as well as retention obligations that might be in place for ongoing litigation or other business or regulatory reasons.

8. Limiting Access to Nonpublic Information

A significant portion of the new regulation is dedicated to protecting and limiting access to nonpublic information. As an initial matter, covered entities must “limit user access privileges to Information Systems” that provide access to nonpublic information. 23 NYCRR 500.07. This requirement dovetails with the regulation’s access-control requirements discussed above.

In addition to limiting access, covered entities must also implement heightened authentication requirements for access to nonpublic information as well as to other sensitive data, systems, and interfaces. “Based on its Risk Assessment,” a covered entity must use “effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication,” to protect against unauthorized access to nonpublic information. 23 NYCRR 500.12. For access to internal systems through an external network, covered entities are required to use multi-factor authentication unless “the Covered Entity’s CISO has approved in writing the use of reasonably equivalent or more secure access controls.” *Id.* This requirement represents a level of regulatory granularity uncommon in the cybersecurity context.

Multi-Factor Authentication: The DFS defines multi-factor authentication (23 NYCRR 500.01(f)) as authentication through at least two of the following types of factors:

- knowledge factors, such as passwords; or
- possession factors, such as a physical token or a text message; or
- inherence factors, including biometric characteristics.

Risk-Based Authentication: The DFS defines risk-based authentication as a system of authentication that detects anomalies or changes in the normal use patterns of a person and requires additional verification of the person’s identity when deviations are detected. 23

NYCRR 500.01(l). For example, a risk-based authentication system would detect when a user attempts to enter his account from a new computer for the first time and would then require the user to answer additional security questions before gaining access.

Encryption: Covered entities must also develop “controls” to protect nonpublic information in transit and at rest. 23 NYCRR 500.15. The “default” measure to protect such information is encryption. If encrypting nonpublic information is not feasible, covered entities may use “alternative compensating controls” to secure the information with the review and approval of the CISO. 23 NYCRR 500.15(a)(1). If an entity chooses to use “alternative compensating controls” rather than encryption, “the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.” 23 NYCRR 500.15(b).

Patterson Belknap Commentary

These requirements are substantial and highly detailed. The requirement to encrypt or otherwise secure nonpublic information both at rest and while in transit may be overly burdensome or difficult to satisfy from a business or operational perspective.

In such cases, “alternative compensating controls” are permitted, but the regulation does not provide further detail or definition of “alternative compensating controls.” Given that, covered entities considering alternatives to encryption may be well-advised to consider the level of protection required for nonpublic information as part of their Risk Assessment.

9. Training and Personnel

Human resources departments and professionals may also feel the weight of the new DFS regulation. Each covered entity must employ sufficient dedicated cybersecurity personnel to manage its cybersecurity risks and “to perform or oversee the performance” of the covered entity’s “core cybersecurity functions.” 23 NYCRR 500.10(a). Those personnel must also receive sufficient training to “address relevant cybersecurity risks” and “maintain current knowledge of changing cybersecurity threats and countermeasures.” *Id.*

The regulation’s training requirements are not limited to cybersecurity personnel. A covered entity must “provide for regular cybersecurity awareness training” for “*all personnel*,” and that training must be “updated to reflect risks” identified in the Risk Assessment. 23 NYCRR 500.14(b) (emphasis added).

Patterson Belknap Commentary

The regulation provides that “all” personnel must receive cybersecurity training. 23 NYCRR 500.14(b). The DFS, however, does not specify the type of training that is appropriate or sufficient. Covered entities may in certain circumstances tailor the training employees receive based on their positions and functions or, in the alternative, consider more generalized training for all employees.

C. Periodic Cyber Risk Assessments

The DFS regulation also requires covered entities to assess and periodically reassess their cybersecurity systems. In addition to the Risk Assessment, the new regulation calls for three different types of regular assessments:

- **Penetration and Vulnerability Testing:** A covered entity must establish programs for “monitoring and testing, developed in accordance” with its Risk Assessment, to assess the “effectiveness” of its Cybersecurity Program. 23 NYCRR 500.05. A covered entity has two “options” for doing so:
 - a. *Continuous Monitoring:* A company may deploy “effective continuous monitoring” (23 NYCRR 500.05), which is not defined in the regulation, and may need to be gleaned from industry standards and practices, as well as the company’s own Risk Assessment.
 - b. *Periodic Assessments:* Instead of continuous monitoring, a covered entity may instead choose to conduct “periodic penetration testing and vulnerability assessments.” 23 NYCRR 500.05. If an organization follows this approach, it must conduct penetration testing annually and vulnerability testing biannually.
 - i. Penetration testing is defined as “a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System.” 23 NYCRR 500.01(h).
 - ii. “Vulnerability assessment” is not defined by the DFS and will likely need to be defined with reference to industry standards and practices.
- **Third-Party Assessments:** Periodically, a covered entity must assess the cybersecurity practices of any third parties that have access to the organization’s network or nonpublic information. 23 NYCRR 500.11(a)(4). The regulation does not define the scope of this assessment, but as a practical matter, this mandate may, depending on the circumstances, apply to payroll and human resource vendors, IT and data-hosting consultants, cloud service providers, and other vendors, consultants, and law firms.

- **Application Security Assessments:** Periodically, the CISO must review, assess, and update procedures and guidelines concerning the security of information system applications. 23 NYCRR 500.08(b). Under the regulation, each organization's Cybersecurity Program must include written procedures, guidelines, and standards to ensure the secure use of internally developed applications. Organizations must also assess and test the security of any externally developed applications that they utilize.

Patterson Belknap Commentary

Because the DFS has not defined "vulnerability assessments" or "third-party assessments," covered entities may in appropriate cases consider the practices of other peer organizations and relevant industry standards as well as their own risk profile when developing such tests.

D. Incident Response Plan

As mentioned above, as part of its Cybersecurity Policy and Program, each covered entity must develop an "incident response plan." 23 NYCRR 500.16. The purpose of the plan, according to the DFS, is to ensure that the organization is prepared to "promptly respond to, and recover from, any Cybersecurity Event affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business." *Id.* The regulation identifies a number of areas that the incident response plan must address:

- the internal processes for responding to a cybersecurity event;
- the goals of the incident response plan;
- the definition of clear roles, responsibilities, and levels of decision-making authority;
- external and internal communications and information sharing;
- remediation of any identified weaknesses in the company's information systems and associate controls;
- documentation and reporting of cybersecurity events; and
- the evaluation and revision of the organization's response plan following a cybersecurity event.

Patterson Belknap Commentary

The DFS regulation itself does not prescribe particular language or details that must be included in an incident response plan. Other governmental agencies have provided guidance that could be informative. For example, the National Institute of Standards and Technology (NIST) framework suggests that organizations predetermine their communication guidelines with “outside parties, such as incident response teams, law enforcement, the media, vendors, and victim organizations.”⁴ NIST also strongly encourages organizations to develop written procedures for prioritizing the handling of individual incidents, including functional and informational factors and detailing recoverability from an incident.⁵ Commentators also encourage organizations to “train, practice, and run simulated breaches to develop response ‘muscle memory.’”⁶

Written policies and procedures for responding to a breach may also provide contemporaneous documentation of readiness, which may be useful for purposes of DFS reviews and in potential litigation or inquiries arising from a breach.

E. Third-Party Information Security Policy

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 IT network or nonpublic information to meet minimum cybersecurity standards. 23 NYCRR 500.11. Specifically, the regulation sets out detailed data security rules and protocols that regulated institutions must impose on all of their vendors and business partners.

Since New York-based banks and insurers are not the only entities covered by the regulation—many out-of-state and foreign institutions that operate in New York under DFS supervision are generally subject to the new regulation as well—the number of third parties affected will be substantial. The DFS’s focus on third parties connected to covered entities is likely a 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 cyber vulnerabilities of vendors with access to company networks.

⁴National Institute of Standards and Technology, Computer Security Incident Handling Guide (2012), page 2, available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.

⁵ Id., page 3.

⁶Tucker Bailey & Josh Brandley, Ten Steps to Planning an Effective Cyber-Incident Response, Harvard Business Review (July 1, 2013), available at <https://hbr.org/2013/07/ten-steps-to-planning-an-effect>.

Under the regulation, covered entities are required to develop and implement written policies and procedures to ensure the security of any IT systems or nonpublic 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 third-party vendors, and create a due-diligence process for evaluating vendors. 23 NYCRR 500.11(a).

Moreover, organizations must establish “relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers.” 23 NYCRR 500.11(b). To “the extent applicable,” those guidelines must address:

- use of multi-factor authentication to limit access to sensitive IT systems or nonpublic information (§500.11(b)(1));
- use of encryption of all nonpublic information—both “in transit and at rest” (§500.11(b)(2));
- notice from the third-party provider to the regulated entity in the event of a breach or potential cyber-related event (§500.11(b)(3)); and
- representations and warranties from third-party provider addressing cybersecurity and policies that relate to the security of the covered entity’s information systems and nonpublic information (§500.11(b)(4)).

In practice, compliance with this aspect of the regulation will require far more than simply “checking the boxes.” Business partners for all covered entities may be required to reconsider their own cybersecurity policies and practices and retool them to comply with the regulation.

Patterson Belknap Commentary

For most organizations, this requirement will be substantial. An April 2015 report by the DFS found that only 46% of surveyed institutions conduct “pre-contract on-site assessments of at least high-risk third-party vendors.” And 44% of those organizations do not require third-party vendors to guarantee that their data and products are free of viruses. Similarly, only half of the surveyed institutions require indemnification clauses for information security failures in their agreements with third-party vendors.

⁷ New York State Dep’t of Fin. Servs., “Update on Cyber Security in the Banking Sector: Third Party Service Providers” (April 2015), page 3, available at http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

⁸ Id., page 5.

⁹ Id., page 6.

As an initial step, covered entities should begin by determining which of their third-party vendors are covered by the regulation and assessing their current contractual arrangements with those vendors. At the same time, a broader third-party vendor program should be contemplated, including, when appropriate, vendor diligence procedures, standard terms and conditions, and provisions requiring prompt notice in the event a vendor suffers a data security incident that might affect the covered entity's nonpublic information or network.

Repeat Obligations Timeline			
Requirement	Annual*	Bi-Annual	"Periodic"
Written Compliance Certificate submitted to DFS	✓		
Risk Assessment			✓
Third Party Assessment			✓
Application Security Assessment			✓
Penetration Testing	✓*		
Chief Information Security Officer Report to Board	✓		
Vulnerability Testing		✓*	

* Penetration Testing must be conducted annually, and Vulnerability Testing bi-annually, absent "effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities."

IV. Additional Requirements

A. Regulatory Reporting

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. 23 NYCRR 500.17(a). Within 72 hours "from a determination" that a cybersecurity event occurred, a covered entity must inform the DFS of the event. *Id.* A cybersecurity event is "material" if it fits within the following categories:

- a cybersecurity event for which notice is required to any other government or self-regulatory agency (§500.17(a)(1)); or
- a cybersecurity event that has a "reasonable likelihood of materially harming any material part of the normal operation(s)" of the covered entity (§500.17(a)(2)).

In addition to reporting cybersecurity events, organizations must certify compliance with the DFS regulation on an annual basis. 23 NYCRR 500.17(b). And every covered entity must maintain "all records, schedules and data supporting this certificate for a period of five years." *Id.*

Patterson Belknap Commentary

The DFS's reporting requirements are, without question, regulatory "firsts" that go beyond regulatory reporting requirements under federal or state laws.

When a cybersecurity event or other triggering circumstance occurs, covered entities now must not only determine whether reporting is required by a federal or state regulator, but must also evaluate whether the event has a "reasonable likelihood of materially harming" the organization's operations. 23 NYCRR 500.17(a)(2).

B. Exemptions

Not every DFS-regulated institution will be subject to all aspects of the regulation. The following types of entities can expect some relief from the regulation's strict requirements.

- Companies with less than \$5 million in gross revenue in New York (in each of the preceding three years), less than \$10 million in year-end total assets from all operations, or fewer than ten employees in New York (including independent contractors) are exempt from a number of the regulation's provisions. 23 NYCRR 500.19(a).
- Companies that do not have information systems and access to nonpublic information are exempt from all but the "Risk Assessment" and "Data Retention" requirements. 23 NYCRR 500.19(c).
- Captive insurance companies—both pure and group captive insurers—are also exempt from all but the "Risk Assessment" and "Data Retention" requirements. 23 NYCRR 500.19(d).
- Finally, charitable annuity societies, risk retention groups not charted in New York, and Rule 125 certified and accredited reinsurers are exempt from the regulation in its entirety. 23 NYCRR 500.19(f).

The first three exempt groups must "file a Notice of Exemption" within thirty days of the "determination that the Covered Entity is exempt." 23 NYCRR 500.19(e). In the event that any Covered Entity, "as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year" to comply with "all applicable requirements" of the regulation. 23 NYCRR 500.19(g).

V. Conclusion

A. Transition Period Timeline

Although the regulation is phased in over a two-year period, most of the requirements must be in place within 180 days. This will require many of the covered institutions to re-examine their overall approach to cybersecurity and determine whether it aligns with the new regulation. We will monitor pertinent developments as institutions roll out their compliance programs and issue regular updates to this publication.

Transition Period Timeline		
Except for the requirement and applicable extended time periods identified below, covered entities will have 180 days from March 1, 2017 to comply with the Regulation.		
One Year	18 Months	Two Years
CISO Report	Audit Trail	Third-Party Service Provider Security Policy
Penetration Testing	Application Security	
Vulnerability Testing	Limitations on Data Retention	
Risk Assessment	User Monitoring	
Multi-Factor Authentication	Encryption	
Regular Cybersecurity Training for All Personnel		

Reproduced with permission from Bloomberg Law: Privacy & Data Security,
<http://www.bna.com/bloomberg-law-privacy-data-security/>.

Copyright © 2017 by The Bureau of National Affairs, Inc., 1801 S. Bell Street, Arlington, VA 22202 (800-372-1033) <http://www.bna.com>.

Privacy Law Watch™

March 21, 2017

Insurance

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

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.

By Craig A. Newman

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.

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.

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 Financial 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, stand-alone 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 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; 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.



Discover the difference.

Costs shouldn't be hidden.
Neither should answers.

- Practical guidance, tools, news and analytics
- Legal and business insights
- The only legal resource for trusted BNA content & Bloomberg News
- Unlimited research at an all-inclusive price

**Bloomberg
Law®**

Learn more about Bloomberg Law
[at bna.com/bloomberglaw](http://bna.com/bloomberglaw)