McDermott Will & Emery

Special Report

New York's Cybersecurity Requirements Pose Multi-Year Compliance Challenges

September 20, 2017

McDermott Will & Emery

SPECIAL REPORT

For more information, please contact your regular McDermott lawyer, or:

Mark E. Schreiber
+ 1 617 535 3982
mschreiber@mwe.com

Michael G. Morgan
+ 1 310 551 9366
mmorgan@mwe.com

Scott A. Weinstein
+1 202 756 8671
sweinstein@mwe.com

Chelsea Hess
+1 212 547 5863
chess@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com

Table of Contents

New York's Cybersecurity Requirements Pose Multi-Year Compliance Challenges

The new cybersecurity regulations issued by the New York State Department of Financial Services (NYDFS) define the nonpublic information they regulate in exceptionally broad terms. This expanded definition of "Nonpublic Information" (NPI) will create major challenges for regulated companies and their third-party service providers that will likely ripple through other ancillary industries.

The regulation's implementation stages are complex and ongoing. NYDFS-regulated entities were required to have a cybersecurity program and detailed NPI safeguards in place as of August 28, 2017. More rigorous implementation stages will follow in 2018 and 2019. Click here for a chart of key compliance dates.

These regulations could be a harbinger of changes beyond New York, as other regulators may consider emulating them in the future.

Challenges Presented by the New Regulations

The expanded definition of NPI goes beyond the current definitions of "personal information" typically used by states in that it includes nonpublic, business-related electronic information if the unauthorized disclosure, access or use thereof would cause a material adverse impact to the business, its operations or security. Covered entities will need to conduct additional risk assessments and consider taking further precautions to protect the security of data sets that contain these additional categories of business information.

Regulated entities whose cybersecurity programs do not already meet these requirements will need to adopt new policies. The regulations take a more prescriptive approach than other regulatory schemes by imposing a series of specific obligations. For example, the regulations require that entities implement controls, including encryption, to protect NPI not only in transit over external networks, but also *at rest*, unless the entity determines that encryption is "infeasible," in which case the entity must implement "alternative compensating controls." This will mean further documentation and justification for the alternative compensating controls, at minimum. The feasibility and value of encryption for data at rest is debatable, and there are a variety of approaches for protecting data at rest.

Some of the obligations have staggered effective dates in 2018 and 2019, making sequencing compliance a challenge. Some later obligations, such as periodic risk assessments and third-party vendor management programs, are not required until March 1, 2018 and 2019, respectively. However, covered entities were required to have considered both to some degree within their cybersecurity programs and policies by August 28, 2017. The progressive nature of these obligations will require constant scrutiny and oversight.

The 72-hour breach notification deadline to the NYDFS Superintendent found in the regulations will present a considerable practical challenge. In many data breaches, it is difficult and time consuming to determine whether a notifiable breach has taken place, and if so, which particular records have been compromised. There are many reasons for this dilemma, including attacker activity (*e.g.*, effective anti-forensic efforts), or the compromise or unavailability of critical log or file data. NYDFS recently provided an online portal for regulated entities to submit breach notifications.[1] Notifications in the 72-hour window are likely to be preliminary at best.

Other regulators may emulate or reinforce the requirements of the regulations. The US Securities and Exchange Commission Office of Compliance Inspections and Examinations, for example, recently announced the outcome of its second cybersecurity examination initiative and recommended that regulated broker dealers, investment advisors and investment companies consider adopting as part of their compliance programs six broad elements[2] that are similar to requirements found in the NYDFS regulation.

---

[1] NYDFS press release announcing online reporting portal, July 31, 2017, at: http://www.dfs.ny.gov/about/press/pr1707311.htm.

[2] Off. of Compliance Inspections & Examinations, US Sec. & Exch. Comm'n., National Exam Program Risk Alert, Vol. 6, Issue 5 (Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-

What Is Required and When?

NYDFS has determined the effective dates of implementation, keyed to section numbers of the regulations, but this material requires some translation. Appendix A at the end of this article summarizes the programmatic requirements and the respective compliance dates in the regulations, as well as the applicability of exemptions, of which there are several.

Who Is Affected?

The regulations apply to any individual or non-governmental entity operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York banking, insurance or financial services law (covered entities), subject to certain exceptions described below.

Who Is Exempt?[3]

A covered entity is exempt from some, but not all, of the requirements in the following instances:

- It has fewer than 10 employees, including independent contractors and employees of affiliates, located in New York or responsible for the covered entity's business.
- It has less than $5 million in gross annual revenue in each of the last three fiscal years from its New York business operations and operations of its affiliates.
- It has less than $10 million in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates (collectively, "size exemptions").

Covered entities whose activities do not involve information systems or NPI are exempt from all but the following requirements ("lack of information exemption")[4]:

- A limitation on data retention
- The requirement to perform a risk assessment
- The requirement to provide the notices to the Superintendent in the case of a cybersecurity event

Finally, certain captive insurance companies that only have access to NPI relating to their corporate parent company are exempt from the same requirements as those covered entities that meet the lack of information systems exemption.[5]

A covered entity that qualifies for an exemption must file a notice of exemption within 30 days of the determination that it is exempt.[6]

What Is NPI?

NPI includes all electronic information in the following categories that is not publicly available:

- Business-related information that, if tampered with or disclosed, accessed or used without authorization, would cause a material adverse impact to the business, operations or security
- Any information concerning an individual that, because of name, number, personal mark or other identifier, can be used to identify such individual in combination with any of the following data elements: social security number, drivers' license number or non-driver identification card number; account number, credit or debit card number; or any security code, access code or password that would permit access to an individual's financial account or biometric records
- Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual that relates to the past, present or future physical, mental or behavioral health condition of any individual or member of the individual's family; the provision of health care to any individual; or payment for

examinations.pdf. The six recommended elements are (1) maintenance of an inventory of data, information and vendors; (2) detailed cybersecurity-related instructions; (3) maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities; (4) established and enforced controls to access data and systems; (5) mandatory employee training; and (6) engaged senior management.

[3] 23 NYCRR § 500.19.

[4] 23 NYCRR § 500.19(c).

[5] 23 NYCRR § 500.19(d).

[6] 23 NYCRR § 500.19(f). The entity must also have determined by Sept. 27, 2017, if it qualifies for an exemption from some or all of the security requirements under the regulations, and must file the required exemption form.

> the provision of health care to any individual[7]

Because this definition includes business-related information, it is quite broad, if not unique. It encompasses more information types than most state data security or data breach notification statutes with respect to "personal information," "personally identifiable information" or "sensitive personal information." As a result, even large corporations that have data security protections in place equivalent to the regulations will have to consider whether those protections apply to all information they store that meets the definition of NPI.

What Is Required as of August 28, 2017?

As of August 28, 2017, covered entities, unless exempted, must meet the following requirements:

- Maintain a cybersecurity program and limit access privileges
- Have implemented and currently maintain a written cybersecurity policy
- Have designated a chief information security officer (CISO) and currently use qualified cybersecurity personnel
- Have established a written incident response plan
- Provide notice to NYDFS of a cybersecurity event[8] within 72 hours

Covered entities have until March 1, 2018, to conduct periodic risk assessments of information systems.[9] However, several elements of the cybersecurity program and policy due August 28, 2017, required the results of a risk assessment, according to the regulation. Therefore, covered entities will have had to complete some aspects of a risk assessment before March 1, 2018.

The NYDFS has clarified, however, that covered entities are generally not required to incorporate provisions for which the applicable transitional period has not yet ended into their cybersecurity programs:

> [W]hile Covered Entities will be required to have a cybersecurity program as well as policies and procedures in place by August 28, 2017, the Department recognizes that in some cases there may be updates and revisions thereafter that incorporate the results of a Risk Assessment later conducted, or other elements of [the Regulation] that are subject to longer transitional periods.[10]

This presumably means that covered entities will not be penalized for certain aspects of their cybersecurity program and policy that may be incomplete, but an iterative review of such programs and policies will be required as the later compliance dates come into effect.

The Risk Assessment[11]

Each covered entity must conduct a periodic risk assessment of its information systems sufficient to inform the design of a cybersecurity program. The risk assessment must be carried out in accordance with written policies and procedures that include the following:

- Criteria for evaluating and categorizing identified cybersecurity risks or threats facing the covered entity
- Criteria for assessing the confidentiality, integrity, security and availability of the covered entity's information systems and NPI,[12] including the adequacy of existing controls in the context of identified risks
- Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks

The risk assessment must be documented and updated as reasonably necessary over time to address changes to the

[7] 23 NYCRR § 500.01.

[8] 23 NYCRR § 500.01(d): Cybersecurity event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.

[9] 23 NYCRR § 500.01(e): Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

[10] *Frequently Asked Questions Regarding 23 NYCRR Part 500*, NY Dep't. of Fin. Serv. (July 31, 2017) http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

[11] 23 NYCRR § 500.09.

[12] 23 NYCRR § 500.01(g).

covered entity's information systems, NPI or business operations, and to permit the covered entity to respond to technological developments and evolving threats.

The Cybersecurity Program[13]

Each covered entity must maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems. The cybersecurity program must be based on the covered entity's risk assessment (described above) and must perform the following functions:

- Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of NPI stored on the covered entity's information systems
- Use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems
- Detect cybersecurity events
- Respond to identified or detected cybersecurity events to mitigate negative effects
- Recover from cybersecurity events and restore normal operations and services
- Fulfill regulatory reporting obligations.

As part of the cybersecurity program, a covered entity must limit user access privileges to information systems that provide access to NPI based on the covered entity's risk assessment and must periodically review such access privileges.[14]

The Cybersecurity Policy[15]

Covered entities must implement and maintain a written policy based on their risk assessment that sets forth their cybersecurity policies and procedures. The policy must address the following items:

- 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 management
- Risk assessment
- Incident response

The policy must be approved by a senior officer[16] or the board of directors.

The Chief Information Security Officer and Cybersecurity Personnel

Each covered entity must designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy. If the covered entity chooses to meet the requirement by using a third-party service provider[17] or an affiliate,[18] the

[13] 23 NYCRR § 500.02.

[14] 23 NYCRR § 500.07.

[15] 23 NYCRR § 500.03.

[16] 23 NYCRR § 500.01(m): Senior officer(s) means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a covered entity.

[17] 23 NYCRR § 500.01(n): Third-party service provider(s) means a person that (1) is not an affiliate of the covered entity; (2) provides services to the covered entity; and (3) maintains, processes or otherwise is permitted access to NPI through its provision of services to the covered entity.

[18] Affiliate means any person that controls, is controlled by, or is under common control with another person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise.

covered entity must retain responsibility for compliance with the regulations, designate a senior member of the covered entity's personnel responsible for direction and oversight of the third-party service provider, and require the third-party service provider to maintain a cybersecurity program that protects the covered entity in accordance with the requirements of the regulation.

The CISO of a covered entity must report on the covered entity's cybersecurity program and material risks in writing at least annually to the covered entity's board of directors, equivalent governing body or a senior officer (if no board of directors or equivalent governing body exists). This annual reporting requirement comes into effect on March 1, 2018.

The CISO (or a qualified designee) must periodically review, assess and update procedures designed to ensure the use of secure development practices for in-house developed applications, and for evaluating the security of externally developed applications utilized within the context of the covered entity's technology environment.[19]

Each covered entity must utilize qualified cybersecurity personnel sufficient to manage the covered entity's cybersecurity risks and to perform or oversee cybersecurity functions.[20] The covered entity must provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks, and must verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. A covered entity may choose to utilize an affiliate or qualified third-party service provider to assist in complying with the cybersecurity requirements set forth in this part of the regulations. There are additional requirements regarding the use of third-party service providers.[21]

Incident Response Plan[22]

Each covered entity shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event materially 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 or operations. The plan must address the following:

- 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
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls
- Documentation and reporting regarding cybersecurity events and related incident response activities
- Evaluation and revision as necessary of the incident response plan following a cybersecurity event

Notices to the Superintendent[23]

Each covered entity must notify New York's Superintendent of Financial Services within 72 hours of a determination that a cybersecurity event has occurred that either (1) affects the covered entity (and where notice of the cybersecurity event is required to any government body, self-regulatory agency or any other supervisory body), or (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity.

A NYDFS FAQ on this subject contains the following information:

> *16. When is a Covered Entity required to report a Cybersecurity Event under 23 NYCRR 500.17(a)?*

[19] 23 NYCRR § 500.08.

[20] 23 NYCRR § 500.10.

[21] 23 NYCRR § 500.11.

[22] 23 NYCRR § 500.16.

[23] 23 NYCRR § 500.17.

23 NYCRR 500.17(a) requires Covered Entities to notify the superintendent of certain Cybersecurity Events as promptly as possible but in no event later than 72 hours from a determination that a reportable Cybersecurity Event has occurred. A Cybersecurity Event is reportable if it falls into at least one of the following categories:

- the Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- the Cybersecurity Event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

An attack on a Covered Entity may constitute a reportable Cybersecurity Event even if the attack is not successful.

The 72-hour notification deadline will present a considerable compliance challenge, as already described. In many breaches, it can take many weeks or months before it is finally determined whether particular data sets are implicated. Nevertheless, it is critical that covered entities take steps now to prepare for the possibility of having to provide notification on very short notice.

Additionally, each covered entity must annually submit a written certification that the covered entity is in compliance with the requirements.

Remaining Requirements Will Soon Be Enforceable

Additional requirements come into effect on March 1, 2018. These include the requirement to continuously monitor or conduct periodic penetration testing [24] and vulnerability assessments to evaluate the effectiveness of the covered entity's cybersecurity program.[25] The covered entity must also provide regular cybersecurity awareness training for all personnel that reflects current risks identified by the covered entity in its risk assessment.[26] Multi-factor authentication must be used for any individual accessing the covered entity's internal networks from an external network, unless the covered entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.[27]

By September 3, 2018, the covered entity must implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, NPI by such authorized users.[28] By that date, the program must include written guidelines and standards designed to ensure the use of secure development practices for in-house developed applications, and procedures for evaluating, assessing or testing the security of externally developed applications utilized within the context of the covered entity's technology environment.[29] It must also include policies and procedures for the secure disposal on a periodic basis of any NPI that is no longer necessary for legitimate business purposes, except where law or regulation otherwise requires such information to be retained, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.[30]

Each covered entity must also implement controls, including encryption, to protect NPI held or transmitted by the covered entity both in transit over external networks and at rest, with the alternative compensating controls if encryption is not feasible. [31] Each covered entity must maintain systems designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the

[24] 23 NYCRR § 500.01(h): Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside the covered entity's information systems.

[25] 23 NYCRR § 500.05.

[26] 23 NYCRR § 500.14(b).

[27] 23 NYCRR § 500.12(c).

[28] 23 NYCRR § 500.14(a).

[29] 23 NYCRR § 500.08.

[30] 23 NYCRR § 500.13.

[31] 23 NYCRR § 500.15.

covered entity.[32] The covered entity must also retain records of these transactions for five years.[33]

Covered entities must also maintain audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity, and must maintain records for at least three years.[34]

Enforcement[35]

The regulations will be enforced by the Superintendent of Financial Services pursuant to the Superintendent's authority under any applicable laws.

Conclusion

The prescriptive nature of these regulations may make them more difficult to comply with than other states' equivalent data security requirements. Even though many covered entities have taken steps in anticipation of the applicability of the regulations, considerable ongoing work will be required to maintain compliance. It remains to be seen whether other state or federal regulatory entities will elect to take a similar approach to the one New York has, and, if they do, whether this will reduce or enhance the flexibility that has come to be a feature in most cybersecurity regulations over the years.

[32] 23 NYCRR § 500.06(a)(1).

[33] 23 NYCRR § 500.06(b).

[34] 23 NYCRR § 500.06(a)(2), (b).

[35] 23 NYCRR § 500.20.

APPENDIX A

Compliance Dates and Requirements with Applicable Exemptions

Compliance Date	Requirement (Citation)	Applicable Exemptions
8/28/17	**Create and maintain a cybersecurity program** § 500.02 **Implement and maintain a written cybersecurity policy** § 500.03 **Limit access privileges** § 500.07	▪ Lack of information exemption ▪ Captive insurance exemption Table
8/28/17	**Designate a chief information security officer** § 500.04(a) **Cybersecurity personnel and intelligence** § 500.10 **Incident response plan** § 500.16	▪ Lack of information exemption ▪ Captive insurance exemption ▪ Size exemptions
8/28/17	**Notice to Superintendent of a cybersecurity event** § 500.17	▪ No exemptions
9/27/17	**Notice to Superintendent of exemptions** § 500.19(e)	▪ No exemptions
2/15/18	**Submit annual report to Superintendent** § 500.17	▪ No exemptions
3/1/18	**Report from chief information security officer** § 500.04(b) **Penetration testing and vulnerability assessments** § 500.05 **Multi-factor authentication** § 500.12 **Regular cybersecurity awareness training** § 500.14(b)	▪ Lack of information exemption ▪ Captive insurance exemption ▪ Size exemptions
3/1/18	**Conduct a periodic risk assessment** § 500.09	▪ No exemptions

9/3/18	**Audit trail** § 500.06 **Application security** § 500.08 **Activity monitoring and detection of unauthorized access** § 500.14(a) **Encryption of nonpublic information** § 500.15	▪ Lack of information exemption ▪ Captive insurance exemption ▪ Size exemptions
9/3/18	**Implement and maintain a data retention policy** § 500.13	▪ No exemptions
3/1/19	**Implement and maintain a vendor management policy** § 500.11	▪ No exemptions

Office Locations

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9-31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
444 West Lake Street, Suite 4000
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: +49 69 271599 633

HOUSTON
1000 Louisiana Street, Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
Heron Tower
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East, 38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas, Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza, Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

ROME
Via A. Ristori, 38
00197 Rome
Italy
Tel: +39 06 462024 1
Fax: +39 06 489062 85

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road, Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, D.C.
The McDermott Building
500 North Capitol Street, N.W.
Washington, D.C. 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087

McDermott
Will & Emery

Boston Brussels Chicago
Düsseldorf Frankfurt Houston London
Los Angeles Miami Milan Munich
New York Orange County Paris Rome
Seoul Silicon Valley Washington, D.C.

Strategic alliance with MWE China Law Offices (Shanghai)

www.mwe.com