New York State Department of Financial Services’ New Cybersecurity Regulation 23 NYCRR Part 500

What You Need to Know to Make Sure Your Insurance Business Complies...

Presented by: NAIFA-NYS, Peter J. Molinaro, Esq. General Counsel
“New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm that is often perpetrated by state sponsored organizations, global terrorist networks, and other criminal enterprises...”

GOV. CUOMO’S PRESS RELEASE 9/13/16
WHO MUST COMPLY?
ARE YOU A COVERED ENTITY?

All Licensed Entities/Persons Must Comply in Some Way With The Provisions of This Regulation

• A “Covered Entity” means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law. [23 NYCRR 500.1(c)]

• “Limited Exemptions” are available for some Covered Entities.
WHAT DATA MUST BE PROTECTED?

The Regulation Is Designed to Protect Nonpublic Information Stored on a Covered Entity’s Information System

*Nonpublic information is defined as:* All electronic information that is not “Publicly Available Information” and is:
1. Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;
2. Any information concerning 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: (i) social security number, (ii) drivers’ license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual’s financial account, or (v) biometric records;
WHAT DATA MUST BE PROTECTED?

3. 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 and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual’s family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care for any individual. [500.01(g)]
A. Each Covered Entity is required to establish and maintain a written cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity’s Information Systems and the Nonpublic Information therein. (500.02)
OVERVIEW OF THE REGULATION

B. Each Covered Entity must adopt and maintain a written cybersecurity policy which contains processes and procedures for data governance and classification, access controls and identity management, business continuity and disaster recovery, systems operation and availability concerns, security, monitoring, quality assurance, privacy, third-party service provider management, risk assessment and incident response. (500.03)
C. Appoint a Chief Information Security Officer (CISO) to oversee implementation and enforcement. (500.04)

D. Supervision and evaluation of cybersecurity program of Third Party Service Providers who have access to Covered Entity’s Information Systems and Nonpublic Information. (500.11)
E. Your Program needs to include a Risk Assessment, use of qualified cybersecurity personnel, timely destruction of unneeded information and an incident response plan. (500.09, 500.10, 500.13, 500.16)

F. Based on the Risk Assessment of your organization, your program may have to include different levels of annual penetration testing with vulnerability assessments, audit trail systems, access logs, review of access privileges, Multi-Factor Authentication for access, employee training and encryption of Nonpublic Information. (500.05, 500.06, 500.07, 500.12, 500.14, 500.15)
THIRD PARTY SERVICE PROVIDER REQUIREMENTS

DEFINITION:

THIRD PARTY SERVICE PROVIDER MEANS A PERSON THAT

(i) is not an Affiliate of the Covered Entity,

(ii) provides services to the Covered Entity, and

(iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity. [500.01(n)]
Based on your Risk Assessment, your program must contain policies and procedures designed to secure your system and Nonpublic Information that is accessible to or in the possession of a Third Party Service Provider. [500.11(a)]
THIRD PARTY SERVICE PROVIDER REQUIREMENTS (continued)

Essentials of Third Party Service Provider Policy: [500.11(a)]

- Identification and risk assessment of the provider
- Minimum cybersecurity practices required to be met by the provider before they conduct their business with the Covered Entity
- Due diligence process used to evaluate the adequacy of the provider’s cybersecurity practices
- Periodic assessment of the provider based on the risk it presents and the continued adequacy of its cybersecurity program

Your program must contain guidelines for the provider’s use of Multi-Factor Authentication, encryption, notice of a Cybersecurity Event to the Covered Entity, representations and warranties to the extent applicable from the provider to the Covered Entity. [500.11(b)]
A Covered Entity Qualifies for a Limited Exemption From Many of the Regulation’s Provisions if That Entity Has One of the Following:

1. Fewer than 10 employees, including independent contractors of the Covered Entity or its affiliates located in New York or responsible for business of the Covered Entity.

2. Less Than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations, including Affiliates

3. Less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of Affiliates. (500.19)
SOME BAD NEWS...

Even if you qualify for the limited exemption, you still have to have:

1. The written cybersecurity program and policy
2. Limited user access privileges
3. Periodic risk assessments
4. Third Party Service Provider supervision and monitoring
5. Secure disposal of no longer needed data
OTHER IMPORTANT EXEMPTIONS...

A. Employees, agents, representatives, designees

B. Affiliates

C. Covered Entities that don’t operate their own system and are not required to keep nonpublic information
OTHER IMPORTANT EXEMPTIONS (continued)...

A. An employee, agent, representative or designee of a Covered Entity, who itself is a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity. [500.19(b)] SUCH EMPLOYEE, AGENT, REPRESENTATIVE OR DESIGNEE OF A COVERED ENTITY IS ALSO EXEMPT FROM DEVELOPING ITS OWN THIRD PARTY INFORMATION SECURITY POLICY IF IT FOLLOWS THE POLICY OF THE COVERED ENTITY WITH WHICH IT WORKS. [500.11(c)]
B. A Covered Entity may meet the requirements of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity. [500.02(c)]
C. A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly Control, own, access, generate, receive or possess Nonpublic Information shall be exempt from all but the Risk Assessment, Third Party Service Provider supervision and monitoring, and data retention provisions of the Regulation. [500.19(c)]
Qualification For The Limited Exemption

• If a Covered Entity qualifies for the exemption, it must file a “Notice of Exemption” in a form provided in Appendix “B” of the Regulation within 30 days of so determining.

• If the entity ceases to qualify for the limited exemption, it shall have 180 days from the end of the fiscal year to comply with all applicable requirements of Part 500.
REPORTING REQUIREMENTS

Annual Report To The Superintendent

• Each Covered Entity shall report annually covering the prior calendar year, by February 15th in a form provided in Appendix “A” of the Regulation, certifying that the Covered Entity is in compliance with the Regulation. [500.17(b)]
REPORTING REQUIREMENTS

Notice Of Cybersecurity Event

• Must notify the Superintendent as promptly as possible but no later than 72 Hours from determining that a “Cybersecurity Event” (as such an event is defined in the Regulation) has occurred. [500.17(a)]
The Following Requirements Must Be Implemented Within the Following Time Frames:

180 Days From The Effective Date or August 28, 2017
1. Cybersecurity Program and Policy Developed
2. Designate Chief Information Security Officer (CISO)
3. Determine System Access Privileges And Personnel Training
4. Establish Incident Response
One Year From The Effective Date or March 1, 2018

1. Complete Risk Assessment and CISO Reports to Governing Body on System Risks
2. Penetration Testing And Vulnerability Assessment
3. Multi-Factor Authentication Program and Awareness Training for All Employees
Eighteen Months From Effective Date or September 1, 2018

1. Audit Trail System Completed and Application Security Written Procedures
2. Policy And Procedures for Disposal of Unneeded Nonpublic Information
3. Encryption of Nonpublic Information
Two Years From Effective Date or March 1, 2019

1. Implement Written Policies and Procedures or Third Party Service Providers
ISSUES YOU MAY BE FACING

• Agent, employee, representative or designee of insurer can be exempt by simply being covered by the insurer’s program. But can this exemption work for independent agents and brokers?

• Even though agents, employees, representatives and designees of insurers are exempt from needing their own program, using the insurer’s program will nonetheless impose difficult cybersecurity requirements.
ISSUES YOU MAY BE FACING

• What types of breaches or attempted breaches arise to the “materiality” standard that requires reporting to the Superintendent within 72 hours?

• How can we adequately comply with the Third-Party Service vendor requirements? Do these requirements limit who we can use to provide needed services? Do we need to include the reg’s requirements in our contract with the vendors?

• Are assets under management considered “assets” for determining qualification for the limited exemption?
NAIFA-NYS ACTION

Filed with NYSDFS comments and critiques to the original draft of this Regulation which was unworkable and did not take into account the needs of our clients.

As a result of our advocacy on your behalf along with over 150 other associations and companies NYSDFS significantly amended the Regulation.
NAIFA-NYS ACTION

Filed additional comments to the current draft of the regulation, but the NYSDFS did not significantly amend the Regulation again before its adoption.

Will continue to discuss the regulation with NYSDFS and express the concerns and issues of our clients during the implementation phase.

Will assist clients with questions about the Regulation and implementation issues.
Questions??
THANK YOU!!!!!!

NAIFA-NYS
17 ELK STREET
ALBANY, NY 12207

518-915-1661  info@naifanys.org