HINMAN STRAUB PC
ATTORNEYS AT LAW

121 State Street
Albany, New York 12207-1693
Tel: 518-436-0751
Fax: 518-436-4751

TO: LeadingAge New York

FROM: Hinman Straub P.C.

RE: Explanation of Proposed Regulation Regarding CyberSecurity

DATE: September 23, 2016

NATURE OF THIS INFORM ATION: This regulation establishes cybersecurity requirements for entities regulated by the Insurance, Banking, and Financial Services Laws.

DATE FOR RESPONSE OR IMPLEMENTATION: Comments on the proposed regulation should be provided to us by November 8, 2016.

HINMAN STRAUB CONTACT PEOPLE: Kelly Ryan, Cheryl Hogan, and Sean Doolan

THE FOLLOWING INFORMATION IS FOR YOUR FILING OR ELECTRONIC RECORDS:
Category: #10 Miscellaneous/Other Suggested Key Word(s):

I. Introduction

The Department of Financial Services has issued a proposed regulation requiring regulated entities to establish cybersecurity programs and policies. The requirements would be applicable to all entities regulated by the Banking Law, the Insurance Law, and the Financial Services Law. The proposed regulation follows up on a series of outreach efforts by the Department to regulated entities and reports summarizing cybersecurity strengths and weaknesses in regulated sectors. The report related to the Insurance Sector was issued in February, 2015 and is available here.

II. Scope and Basic Requirements

The proposed regulation applies to "covered entities" which are defined broadly as "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." There is a limited exemption for covered entities with fewer than 1000 customers in each of the last three calendar years, less than $5 million in gross annual revenue for each of the last three fiscal years, and less than $10 million in year-end total assets. With respect to insurance, we believe that in addition to insurers, agent, brokers, and utilization review agents would be subject to the regulation.

In general, the definitions in the regulation are fairly standard. However, the term "cybersecurity event" is broadly defined as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an IT system or information stored on an IT system. No exclusion for "pings" is included as it is in the HIPAA Security Rule. The term "nonpublic information" is defined as "any information that is not Publically Available Information and is:

- Any business related information which would cause a material adverse impact to the business, operations, or security of the covered entity if tampered with;
- Any information provided by an individual to a covered entity in connection with the seeking or obtaining of any financial product or service, or information about an individual resulting from a transaction, or information obtained about the individual in connection with providing a financial product or service;
- Any information, except age and gender, that is created by, derived or obtained from a health care provider or any individual that relates to the past, present, or future physical, mental, or behavioral health or condition of any individual or member of the individual's family or household, or from the provision of or payment for health care;
- Any information used to distinguish or trance an individual's identity or any information that is linked or linkable to an individual, including but not limited to medical, educational, financial, occupational, or employment information, information about an individual used for marketing purposes or any password or other authentication factor.

The proposed regulation would be effective January 1, 2017 and covered entities would have until July 1, 2017 to comply with the requirements. The first annual report, as described below, would be due January 15, 2018.

III. Cybersecurity Policy

Under the proposed regulation, covered entities must implement and maintain a written cybersecurity policy. The policy must be fairly comprehensive and address, at a minimum:

1. Information security;
2. Data governance and classification;
3. Access controls and identity management;
4. Business continuity and disaster recovery planning resources;
5. Capacity and performance planning;
6. Systems operations and availability concerns;
7. Systems and network security;
8. Systems and network monitoring;
9. Systems and application development and quality assurance;
10. Physical security and environmental controls;
11. Custom data privacy;
12. Vendor and third-party service provider management;
13. Risk assessment; and
14. Incident response

The covered entity's Board of Directors must review the policy and it must be approved by a senior officer as often as necessary, but at least annually.

Health insurers are already required by the HIPAA Security Rule to maintain comprehensive security policies that include the elements listed above.

IV. Cybersecurity Program

Covered entities would be required to establish and maintain a cybersecurity program that ensures the confidentiality and integrity of covered entities' IT systems. At a minimum, the program must:

- Identify internal and external cyber risks by, at a minimum, identifying nonpublic information stored on its systems, the sensitivity of such nonpublic information, and how and by whom it may be accessed;
- Use a defensive infrastructure and the implementation of policies and procedures to protect information systems and nonpublic information from unauthorized access, use, or other malicious acts;
- Detect cyber security events;
- Respond to identified or detected cybersecurity events to mitigate any negative effects;
- Recover from cybersecurity events and restores normal operations and services; and
- Fulfill all regulatory reporting obligations.

The cybersecurity program must include the following elements, which are further described below:

1. Penetration testing
2. Audit trail
3. Access privileges
4. Application security
5. Limits on data retention
6. Training and monitoring
7. Encryption
8. Incident response plan

A. Penetration Testing

The cybersecurity program must include annual penetration testing and quarterly vulnerability assessments. The survey conducted by the Department indicates that 100% of insurers surveyed conduct penetration testing, but the frequency of that testing varies significantly. Still, the overwhelming majority of insurers surveyed conduct the test at least annually.

B. Audit Trail

The cybersecurity program must include implementation and maintenance of an audit trail system. At a minimum, this system must:

- Track and maintain data that will allow the complete and accurate reconstruction of all financial transactions and accounting necessary to detect and respond to a cybersecurity event;
- Track and maintain logs of all privileged authorized user access to critical systems;
- Protect the integrity of data stored and maintained as part of any audit trail from alteration or tampering;
- Protect the integrity of hardware from alteration or tampering, including limiting electronic and physical access permissions;
- Log system events including, at a minimum, access and alterations made to the audit trail systems by the systems or by an authorized user, and all system administrator functions performed on the systems; and
- Maintain records produced as part of the audit trail for not fewer than six years.

C. Access Privileges

Covered entities must limit access to IT systems that provide access to nonpublic information to individuals who require such access in order to perform their responsibilities. Such access privileges must be periodically reviewed.

D. Application Security

The cybersecurity program must include written procedures, guidelines, and standards to ensure that in-house developed applications are developed securely, as well as procedures for assessing and testing the security of all externally-developed applications used by the covered entity.

These procedures, guidelines, and standards must be reviewed, assessed, and updated by the Chief Information Security Officer at least annually.

E. Data Retention

The cybersecurity program must include policies and procedures pursuant to which nonpublic information that is no longer needed for the purpose for which it was provided is timely destroyed, unless the information is required to be maintained pursuant to law or regulation.

F. Training and Monitoring

Covered entities must implement risk-based policies, procedures, and controls to monitor the activity of authorized users to detect unauthorized access or use of nonpublic information by authorized users.

Additionally, covered entities must require all personnel to attend regular cybersecurity awareness training sessions provided for by the covered entity. The trainings must be updated to reflect risks identified by the covered entity in its annual risk assessment.

G. Encryption

Covered entities must encrypt all nonpublic information held or transmitted both in transit and at rest. If encryption is currently infeasible, covered entities may secure nonpublic information using appropriate alternative compensating controls. This flexibility expires as it relates to information in transit one year after the regulation becomes effective and five years after the regulation becomes effective with respect to encryption of information at rest.

H. Incident Response Plan

A covered entity must establish and maintain a written incident response plan as part of its cybersecurity program. The response plan must be designed to promptly respond to, and recover from a cybersecurity event affecting the confidentiality, integrity, or availability of the covered entity's IT systems, or the continuing functionality of any aspect of the covered entity's business. The plan must, at a minimum, 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 information systems and associated controls;
- Documentation and reporting regarding cybersecurity events and related response activities; and
- The evaluation and revision of the response plan following a cybersecurity event.

V. Information Security Officer and Personnel

Each covered entity must designate a qualified individual to serve as the Chief Information Security Officer (CISO). This individual is responsible for the implementation of the cybersecurity program and enforcement of the cybersecurity policy. Covered entities may delegate this function to a third party, but must maintain ultimate responsibility for compliance and must designate a senior employee to oversee the third party. The CISO must deliver a report at least bi-annually to the Board of Directors. The report must:

- Assess the confidentiality, integrity and availability of information systems;
- Detail exceptions to cybersecurity policies and procedures;
- Identify cyber risks;
- Assess the effectiveness of the cybersecurity program;
- Propose steps to remediate any inadequacies identified;
- Include a summary of all material cybersecurity events that affected the covered entity during the time period addressed by the report.

Additionally, a covered entity must employ cybersecurity personnel sufficient to manage the cybersecurity risks faced by the entity and to perform core cybersecurity functions required by the regulation. These individuals must attend regular training sessions and stay abreast of changing threats and countermeasures. The survey conducted by the Department found that more than half of surveyed insurers outsource at least some of their IT systems management. A covered entity may choose to engage a third party to assist with compliance, but must comply with third party requirements discussed in further detail in Section VII below.

VI. Risk Assessment

A risk assessment of the covered entity's IT systems must be conducted at least annually. Written policies and procedures must govern the risk assessment, and must include criteria for the evaluation and categorization of identified risks; criteria for the assessment of the confidentiality, integrity and availability of the covered entity's IT systems, including the adequacy of existing controls in the context of identified risks; and requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks. The outcome of the risk assessment must be documented in writing.

VII. Third Party Information Security Policy

Covered entities must implement written policies and procedures that are designed to ensure the security of IT systems and nonpublic information accessible to, or held by, third parties with which the covered entity is doing business (e.g., Business Associates). At a minimum, such policies and procedures must address:

- Identification and risk assessment of third parties covered by the requirements;
- Minimum cybersecurity requirements that must be met by third parties;

- Due diligence processes used to evaluate the adequacy of cybersecurity practices of third parties; and
- Assessment of third parties and the adequacy of their cybersecurity policies on a periodic basis, but no less than annually.

The policies and procedures must also provide for the establishment of preferred third party contract provisions, including provisions addressing multi-factor authentication; use of encryption; prompt notice to the covered entity of a security event (this is already required under HIPAA); identity protection services for customers materially impacted by a security event due to the third party's negligence or misconduct; representations and warranties by the third party that its service or product is free from viruses, etc. that would impair the security of the covered entity's IT systems or non-public information; and the right of the covered entity to audit the third party.

VIII. Authentication Requirements

Covered entities must require multi-factor authentication for any individual accessing internal systems or data from an external network and for privileged access to database servers that allow access to nonpublic information. "Multi-factor authentication" means authentication through at least two of the following factors:

- Knowledge factors (e.g., passwords);
- Possession factors (e.g., token or text message)
- Inherence factors (e.g., biometrics)

To access web applications that capture, display, or interface with nonpublic information, covered entities must require "risk-based authentication," which detects anomalies or changes in the normal use patterns of a person and requires additional verification of identity when deviations are detected (e.g., through the use of challenge questions). Multi-factor authentication must be supported to access such web applications, but is not required.

IX. Notice to Superintendent

In addition to existing requirements related to reporting security breaches and similar incidents, the proposed regulation would require a covered entity to notify the Superintendent of any cybersecurity event that "has a reasonable likelihood of materially affecting the normal operation of the entity or that affects nonpublic information." This notice must be provided as promptly as possible, but no later than 72 hours after becoming aware of the event. This notice requirement applies to any event that must be reported to any government or self-regulatory agency and any event that involves the actual or potential unauthorized tampering with, access to, or use of nonpublic information.

In addition, covered entities must annually file a written statement with the Superintendent certifying compliance with the requirements of the regulation. An example of the attestation is included with the draft regulations and the form must be filed by January 15 of each year. Related records, schedules and data must be maintained for five years.

In the event weaknesses have been identified that require material improvement, updating or redesign, Covered entities must document such plans and efforts and maintain this documentation for inspection by the Superintendent. If a material risk of imminent harm is identified, the Covered Entity must notify the Superintendent within 72 hours and include reference to such items in its annual report.

X. Draft NAIC Data Security Model Law

While the proposed regulation is similar in some respects to the NAIC's draft data security model law, the NAIC draft law is more comprehensive. Specifically, the NAIC draft law includes a number of provisions related to breaches and consumer protections following a breach, while the proposed regulation does not address these issues.

With respect to the establishment of a data security program, the NAIC draft law offers some additional flexibility as compared to the proposed regulation because it takes into account the size and complexity of the licensee, the nature and scope of the licensee's activities, and the sensitivity of the personal information in the licensee's possession, custody or control in establishing a data security program, which the proposed regulation does not. In other respects, the requirements for data security programs are similar.