The following article is from National Underwriter's latest online resource,
FC&S Legal: The Insurance Coverage Law Information Center.

FC&S LEGAL
The Insurance Coverage Law Information Center

NEW YORK ANNOUNCES REVISIONS AND DELAYED IMPLEMENTATION OF CYBER REGULATIONS

January 17, 2017

Benjamin P. Malerba and Ada Kozicz

In September 2016, New York Governor Andrew Cuomo announced a new regulation that would require insurers and banks to implement cyber security programs. Specifically, the proposed regulation required covered entities, defined as any entity operating under a license or other authorization required by New York's banking, insurance or financial services law, to establish and maintain a cyber security program that would protect the confidentiality, integrity and availability of the covered entity's information systems. This regulation was initially intended to take effect on January 1, 2017. However, on December 28, 2016, after reviewing over 150 comments submitted by the public, the New York Department of Financial Services ("DFS") decided to revise the proposed regulation and delay its implementation until March 1, 2017.

The Proposed Regulation

Under the revised regulation,[1] covered entities will be required to conduct a risk assessment on a periodic basis to ensure that they have an effective cyber security program and to update the program as reasonably necessary to address changes in technology, business operations, and evolving threats to the entity's information systems. The proposed regulation originally required cyber security programs to address all of the following areas:

- information security;
- data governance and classification;
- access controls and identity management;
- business continuity and disaster recovery planning and resources;
- capacity and performance planning;
- 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; and
- incident response.

Additional Revisions

The revised regulation, however, offers more flexibility by allowing each covered entity to tailor its cyber security program based on the risk assessment of its cyber security threats and protective measures. The areas listed above must only be included in the cyber security program to the extent they are applicable to the entity's business operations. The revised regulation also added "asset inventory and device management" to the list of areas that may be included in an effective cyber security program, if applicable. Other revisions to the proposed regulation include:

- *Clarification that the Chief Information Systems Officer ("CISCO"), appointed to manage a covered entity's cyber security program does not have to be exclusively dedicated to CISCO activities.*
    - Any existing employee of a covered entity that is qualified to perform CISCO activities may be appointed as the CISCO and may perform such activities in conjunction with his or her other job responsibilities. Alternatively, the CISCO can be an employee of an affiliate or third-party service provider of the covered entity.
- *Addition of an exception to the limitation on data retention.*
    - Under the new exception, a covered entity is not required to dispose of nonpublic information that is no longer necessary for business operations if such information is otherwise required to be retained by law or if the disposal of such information is not reasonably feasible because of the manner in which it is maintained.
- *Deletion of any language that unintentionally suggested that covered entities are required to audit the information systems of their third party service providers.*
    - However, covered entities will still be required to implement policies and procedures that protect nonpublic information that is accessible to any third parties that provide services to the covered entity.
- *Revisions to the 72-hour reporting requirement when a cyber security event occurs.*
    - Although many public comments expressed concern that 72 hours is not enough time to collect information and assess a potential cyber security event, DFS did not increase this timeframe for reporting a cyber security event to DFS. However, the revised regulation explains that a covered entity must only report an event within 72 hours if it determines that the event has a reasonable likelihood of materially harming a material part of its business operations.
- *Addition of exemptions for small businesses in order to reduce the financial burden of complying with some of the requirements under the new regulation.*
    - Small businesses with (i) less than 10 employees, including independent contractors; (ii) less than $5,000,000 in gross annual revenue in the past three fiscal years; or (iii) less than $10,000,000 in year-end total assets, including assets of all affiliates, must still conduct a period risk assessment and implement a cyber security program, but are exempt from complying with the following requirements:

    (a) utilizing a multi-factor authentication system to protect its information systems from unauthorized access;

    (b) appointing a CISCO to manage the cyber security program;

    (c) using qualified cyber security personnel to manage cyber security risks and protective measures;

    (d) training personnel based on risk assessment results;

    (e) encrypting all nonpublic information; and

    (f) establishing a written incident response plan.

    - In addition, an employee, agent or representative of a covered entity that is itself a covered entity is exempt from developing its own cyber security program if its business operations are covered under the cyber security program of the covered entity for which it provides services. All covered entities that are exempt under the revised regulation must file a Notice of Exemption with DFS.

Public Comments and Effective Date

The revised regulation is subject to an additional 30-day public comment period, but DFS will only respond to comments that raise new issues and questions. Unless DFS decides to make further revisions based on the new comments it receives, the regulation will take effect on March 1, 2017. Thereafter, covered entities have 180 days to comply with the regulation. However, the regulation also provides a transition period whereby covered entities will have an extended timeframe to comply with certain requirements in order to reduce their financial and administrative burden. For example, covered entities will have one year to conduct a risk assessment, obtain a multi-factor authentication system and train personnel on their cyber security program. They will have 18 months to encrypt all nonpublic information and to dispose of any nonpublic information that is no longer needed for business operations (unless an exception applies). Finally, covered entities will have two years to establish written policies and procedures that are designed to protect nonpublic information that is accessible to or held by third party service providers.

Annual Certification

All covered entities will be required to certify with DFS on an annual basis that they have complied with the regulation and have maintained an effective cyber security program. The first annual certification will be due to DFS on February 15, 2018. DFS will likely issue additional guidance on complying with the new regulation in the near future.

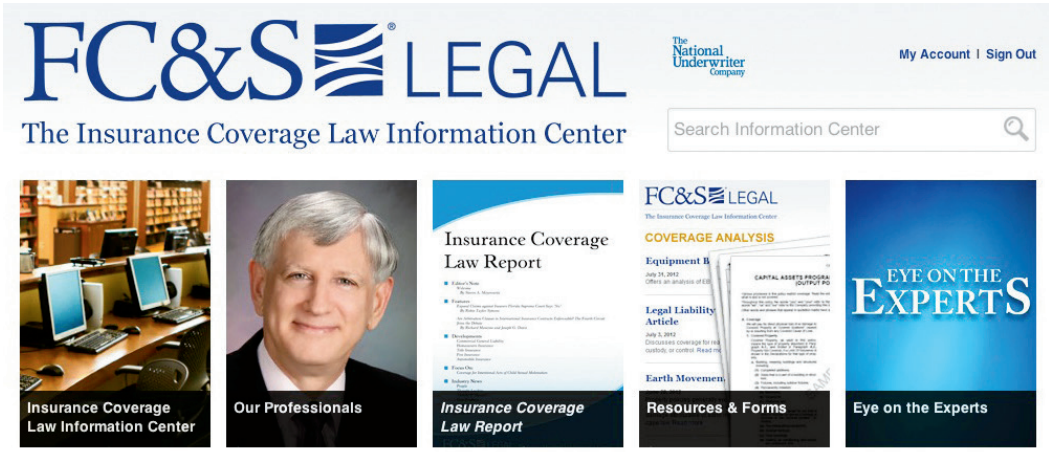
Note

[1] The revised regulation is available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

About the Authors

Benjamin P. Malerba is a partner in the Health Services and Privacy, Data & Cyber Law Practice Groups at **Rivkin Radler LLP** focusing his practice on data breach and response, cybersecurity and data security, with a particular focus on Health Insurance Portability and Accountability Act of 1996 (HIPAA) related security breaches. He counsels clients on the development and implementation of compliance programs for healthcare providers and business associates under HIPAA and on preparing for and responding to HIPAA breaches and investigations. Mr. Malerba may be reached at benjamin.malerba@rivkin.com.

Ada Kozicz is an associate in **Rivkin Radler LLP**'s Health Services and Privacy, Data & Cyber Law Practice Groups concentrating her practice on regulatory and transactional matters within the healthcare industry. She also advises clients both in and outside of the health care industry on complying with HIPAA and the HITECH Act and responding to any threats or breaches to an organization's privacy and cyber security. Ms. Kozicz may be reached at ada.kozicz@rivkin.com.



For more information, or to begin your free trial:

- Call: 1-800-543-0874
- Email: customerservice@nuco.coms
- Online: www.fcandslegal.com

FC&S Legal guarantees you instant access to the most authoritative and comprehensive insurance coverage law information available today.

This powerful, up-to-the-minute online resource enables you to stay apprised of the latest developments through your desktop, laptop, tablet, or smart phone —whenever and wherever you need it.

NOTE: The content posted to this account from ***FC&S Legal: The Insurance Coverage Law Information Center*** is current to the date of its initial publication. There may have been further developments of the issues discussed since the original publication.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service. If legal advice is required, the services of a competent professional person should be sought.

Copyright © 2017 The National Underwriter Company. All Rights Reserved.