Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

MARCH 2017

Department of Financial Services Issues Final Cybersecurity Regulations With Broad Implications for Health Plans and Health Care Providers

On February 16, 2017, the New York State Department of Financial Services ("DFS") issued final cybersecurity regulations, with extensive new requirements for cybersecurity programs by entities regulated by DFS ("Covered Entities"), including banks, insurance companies, and health plans supervised by DFS ("Final Regulations"). The Final Regulations respond to criticism of the proposed regulations, which were issued first on September 13, 2016, and again on December 28, 2016, but retain many key elements of the regulations as initially proposed. With an effective date of March 1, 2017, the Final Regulations phase in certain obligations, over a time period ranging from six months to two years.

The Final Regulations cover health plans directly, and will impact health care providers as health plan contractors. Among other provisions that mandate increased cybersecurity measures, the regulations, as initially released and as issued in final form, require health plans and other Covered Entities to: (i) set minimum standards for the security practices of third party contractors they do business with; (ii) adopt due diligence processes to evaluate third party security practices; and (iii) periodically assess third parties based on the risk they present to nonpublic covered information ("NPI"), defined to include medical information. The Final Regulations are far more prescriptive than the Health Insurance Portability and Accountability Act ("HIPAA") and will impose new obligations on health plans, and on health care providers as third party contractors.

The Final Regulations apply to all organizations that hold a license, permit, registration charter, certificate, accreditation or similar authorization under the Banking Law, Insurance Law or Financial Services Law, unless an exemption applies. Among the most significant changes made in the Final Regulations is the grant of an exemption for hundreds of colleges and universities, large health systems, hospitals, and other not-for-profit organizations in the State covered by the proposed regulations due solely to the fact that they have a permit from DFS for a donor annuity program. (See January 2016 letter by Tracy Miller, joined by the Commission on Independent Colleges and Universities, urging DFS to exempt institutions of higher education and other not-for-profit organizations; for further discussion of the exemption, see Bond Memo.)

I. Regulatory Mandates

Among other provisions, the Final Regulations require Covered Entities to:

- Adopt a cybersecurity program with specified elements;
- Designate a qualified individual to serve as a chief information security officer responsible for overseeing, implementing and enforcing the cybersecurity program and policy;
- Adopt policies and procedures for the security of information systems and NPI accessible to or held by third parties;
- Address data governance and classification, to the extent applicable;
- Address systems and application development and quality assurance, as applicable;
- Conduct continuous monitoring or annual periodic penetration testing and a bi-annual vulnerability assessment;
- Maintain audit systems to detect and respond to cybersecurity events;
- Use multi-factor or risk-based authentication;
- Encrypt NPI at rest and in transmission; and
- Adopt an incident response plan with specified elements.

In response to public criticism, the Final Regulations qualified certain of the specified elements of a cybersecurity program by stating that the requirements would apply based on the risk assessment conducted by the Covered Entity, rather than applying uniformly to all Covered Entities. Reflecting the increasing focus on board and senior management accountability for cybersecurity, the board of directors or a senior officer of each Covered Entity must submit a certificate of compliance with the Final Regulations on an annual basis starting on February 15, 2018.

Covered Entities with fewer than ten (10) employees or less than $5 million gross annual revenue for three years, or less than $10 million in year-end total assets, will be exempt from a subset of the Final Regulations. In addition, Covered Entities that do not operate, maintain, utilize or control any information systems or do not control, own, access, generate, receive or possess NPI will also be exempt.

II. Requirements Applicable to Third Party Service Providers

Under the Final Regulations, Covered Entities are required to implement written policies and procedures governing their practices with respect to third party service providers that access NPI ("Contractors") based on the Covered Entity's risk assessment. Specifically, as set forth in the Final Regulations, Covered Entities, including health plans, must adopt policies that address:

- Identification and risk assessment of Contractors;
- Minimum security practices that must be met by Contractors in order to do business with the Covered Entity;
- Procedures for due diligence to evaluate the adequacy of Contractors' security practices; and
- Guidelines for contractual protections relating to Contractors' access to NPI.

Consistent with a risk assessment by the Covered Entity, such policies must address procedures for access control, including multi-factor identification, encryption of information in transit and at rest, and practices to notify the Covered Entity of a cybersecurity event that directly impacts the Covered Entity's information systems and NPI. Guidelines must also cover the representations and warranties that Contractors will extend to the Covered Entity regarding their cybersecurity policies, although the Final Regulations are less prescriptive about the specific elements of such representations and warranties then the proposed regulations. The Final Regulations grant health plans and other Covered Entities two (2) years to adopt these third party contracting requirements.

III. Cybersecurity Event Reporting

Under the Final Regulations, Covered Entities must report cybersecurity events, as defined in the Final Regulations, to DFS as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred, defined as events where: (i) entities are required to provide notice to another governmental or supervisory body; and (ii) events that have a reasonable likelihood of harming any material part of the normal operations of the Covered Entity. As a result, all breaches that must be reported to the Department of Health and Human Services ("HHS") under HIPAA or the New York State Attorney General under New York State's breach notification law must also be reported to DFS.

IV. DFS Final Regulations and HIPAA—New Demands for Health Plans and Health Care Providers

Designed principally for banks, insurance companies, and other financial institutions regulated by DFS, the Final Regulations will impose new demands on health plans, and indirectly on health care providers as third party contractors. One of the earliest regulations governing cybersecurity, the HIPAA Security Rule is scalable; it does not specify technology requirements, with the exception of the standards for encryption that must be met to determine whether a breach has occurred and must be reported. In accordance with the HIPAA Security Rule, security programs must be reasonable in light of the size and capacities of each organization. Other major security laws, including the Gramm-Leach-Bliley Act, have followed suit, adopting flexible standards for technical safeguards and solutions.

The Final Regulations take a different approach. While recognizing that a security program should be based on a risk assessment, the Final Regulations enumerate many technical safeguards and standards that must be considered or adopted, including: (i) continuous monitoring or annual penetration testing and bi-annual vulnerability assessment; (ii) verification that cybersecurity personnel take steps to maintain knowledge of changing cybersecurity threats and countermeasures; and (iii) encryption for NPI not only in transmission but at rest. The annual certification by the Board of Directors or senior officer that the organization is in compliance is also a significant additional mandate.

Reporting standards are entirely distinct under the Final Regulations in terms of the criteria and time frame for reporting. Under HIPAA, covered entities must report a breach of unsecured protected health information that affects 500 or more individuals to the Secretary of HHS, without unreasonable delay, but no later than 60 days following discovery of the breach. HIPAA enumerates certain exceptions to reporting, including instances where the covered entity determines that there is a low probability that protected health information was compromised based on a risk assessment. The Final Regulations require a breach report to DFS as promptly as possible, but no later than 72 hours from a determination that a reportable event has occurred. Given that one basis for a reportable event is the duty to report to another governmental body, the time frame for reporting under the Final Regulations is aligned with the time frame under HIPAA, at least in cases where the basis for reporting is the duty to report to another governmental body. In other cases, a breach report will have to meet the more stringent time period imposed by the Final Regulations.

The Final Regulations are also likely to impose substantial new obligations on health care providers as third party contractors of health plans. Under HIPAA, covered entities must bind third parties that will receive PHI to comply with HIPAA in a Business Associate Agreement. While those agreements may specify security safeguards, HIPAA does not mandate technical safeguards or solutions for review or consideration. The Final Regulations require health plans, among other Covered Entities, to set minimum security requirements and to assess access controls, including multi-factor authentication.

Health care providers potentially will be subject to differing standards as adopted by health plans, in a regulatory scheme that focuses on technical solutions rather than the size or resources of organizations. For that reason, the Final Regulations may prove particularly problematic for smaller health care providers. The two (2)-year lag in the implementation date of the third party contract provisions will provide some relief, but implementation is still likely to prove costly and complex for many health plans and providers.

For questions about the Final Regulations or further information, contact Tracy E. Miller, Deputy Chair, Health Care and Long-Term Care Practice, and Co-Chair of the Cybersecurity and Data Privacy Practice.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond