ALERT

23 NYCRR Part 500 (Cybersecurity Regulation) CCRC Update

DECEMBER 2018

Regulation 23 NYCRR Part 500 (cybersecurity regulation) was issued by the New York State Department of Financial Services (DFS) in March of 2017. DFS stated in writing on February 28, 2018 that Continuing Care Retirement Communities (CCRC) are covered by the requirement. An effort in the Senate, proposed to amend the insurance law, in relation to authorizing CCRCs to adopt a written cybersecurity policy rather than complete the required full attestation. The purpose of the bill was to permit CCRCs to attest to the DFS that the CCRC's cybersecurity policies are not inconsistent with cybersecurity regulations promulgated by the superintendent. The bill was approved, unanimously, by the Insurance Committee and the Rule Committee. On December 7, 2018 the Governor vetoed the bill. DFS's position regarding compliance has remained constant:

All CCRCs that failed to submit the Certification but **are in compliance** with the regulation should do so via the DFS cybersecurity portal **as soon as possible.** *"…The DFS Certification of Compliance is a critical governance pillar for the cybersecurity program of DFS regulated entities, and DFS takes compliance with the regulation seriously. The Department will consider a failure to submit a Certification of Compliance as an indicator that the cybersecurity program of the Covered Entity has a substantive deficiency."*

We interpret this to mean that any entity that has not complied with the regulation should take the necessary steps to become compliant as soon as possible.

WHAT DOES THE REGULATION REQUIRE?

The regulation stipulates that covered entities meet the following requirements:

- Assess whether the risk assessment program adequately addresses cybersecurity risks and that the outputs from such assessments are used in the cybersecurity program management.
- Assess the cybersecurity policy to determine whether it adequately addresses the regulation's requirements.
- Assess whether the cybersecurity program, based on a risk assessment, sufficiently addresses the regulation's requirements related confidentiality, integrity and availability aspects.
- Assess the approach to addressing the regulation's requirement for a Chief Information Security Officer.
- Assess the current business continuity and recovery plan and its ability to maintain security audit trails to determine compliance with the regulation's requirements.
- Assess the user access provisioning and access maintenance policies, procedures and controls.
- Assess the software acquisition, development and change management policies, procedures and controls to determine whether cybersecurity requirements are adequately addressed.
- Assess whether the organization utilizes qualified and competent personnel to develop, implement, maintain and enforce its cybersecurity program and requirements.
- Assess the third party risk management program to determine whether it adequately addresses cybersecurity risks.
- Determine whether the organization adequately addresses the multifactor authentication requirements.
- Assess the data retention and disposal policy, procedures and controls.
- Assess the approach to cybersecurity training and monitoring.
- Assess the approach to encrypting non-public information.
- Assess the quality of the incident response plan.

WHEN DO I NEED TO COMPLY?

The recent actions by the Governor do not change the fact that covered entities are required to comply with the timeline as originally prescribed in the regulation. DFS has stated that attestations should be submitted "as soon as possible". It should also be noted that the two year transition period ends on March 1, 2019 so all elements of Regulation 23 NYCRR part 500 will be required to be complied with under the regulation as currently written by that date. In our opinion non-compliant organizations should take these regulations seriously and ensure compliance as quickly as is reasonably possible.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

The regulation does not specifically detail penalties for non-compliance. The regulation states "This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws". Absent any specific guidance it is reasonable to assume that enforcement actions could arise pursuant to the general authority of DFS under the NY Banking law, which allows the superintendent of DFS to require a regulated entity to pay a penalty "for any violation of any regulation promulgated:. NY Banking law authorizes up to (1) $2,500 per day during which a violation continues (b) $15,000 per day in the event of any reckless or unsound practice or pattern of miscount, or (c) $75,000 per day in the event of a knowing and willful violation.

HOW CAN FREED MAXICK HELP?

At Freed Maxick we understand that some CCRCs may be challenged to implement the full complement of security policies and procedures required by the regulation.

A Cybersecurity Assessment completed by our certified security analysts can provide an evaluation of which areas of the DFS regulations an organization currently complies with, and which areas it could improve upon and doesn't meet. This assessment has the ability to examine the organization's current security posture in alignment with the NIST Cybersecurity Framework (CSF), as well as the controls examined in the DFS 23 NYCRR Part 500 document. We will review the results of the assessment with the organization to provide insight into next steps on how to meet the compliance areas in question.

Freed Maxick approach to execute the Cybersecurity Assessment includes:

- Meeting with subject matter experts to obtain documentation and interview responses that will help build the assessment plan
- Conducting internal and external vulnerability scanning to locate vulnerabilities potentially opening the organization to cyber threats
- Analyzing results of the assessment and providing a report with the assessment results summarized
- Development of POA&Ms (Plans of Actions and Milestones) that will assist system owners in properly handling identified system deficiencies

Our cybersecurity professionals are available to help assess your current state and help you remediate any gaps to achieve compliance with all regulatory requirements of the DFS 23 NYCRR Part 500 document.

WHO NEEDS TO COMPLETE THE ATTESTATION?

The attestation should be completed by either the board of directors or a senior officer of the covered entity.
A copy of the required attestation is on the following page.

Example Attestation

(Covered Entity Name)

February 15, 20__

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of _____ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended (year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date: _____

FOR ADDITIONAL INFORMATION CONTACT:

Chris Eckert, CPA
Director - Healthcare
christopher.eckert@freedmaxick.com
716.332.2656

Sanath Rajapakse
Director - Risk Advisory Services
sanath.rajapakse@freedmaxick.com
716.332.2629