CARLTON FIELDS

NAIC Cybersecurity Working Group Votes to Approve Insurance Data Security Model Law

September 26, 2017

The National Association of Insurance Commissioners (NAIC) Cybersecurity (EX) Working Group (Cybersecurity WG) approved Version 6 (Finalized) of its Insurance Data Security Model Law (Model) on August 7 at the NAIC Summer 2017 National Meeting in Philadelphia. The following day the Model was approved by the Innovation and Technology Task Force. Next, it will be considered by the NAIC Executive Committee, and if approved, sent to the Joint Meeting of the Executive Committee and Plenary for vote by all NAIC Members. Version 6 of the Model incorporates significant changes from the first version released March 2, 2016, including the narrowed purpose of establishing "standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to licensees…" The Model applies to all licensees, defined as individuals or non-governmental entities required to be authorized, registered, or licensed pursuant to a state's insurance laws. There are very limited exceptions to the definition. The Model also requires that all licensees develop, implement, and maintain a comprehensive written Information Security Program (ISP). The ISP should be based on an individual risk assessment and be commensurate with the licensee's size and complexity, the nature and scope of its activities, and the sensitivity of the nonpublic information used or in the licensee's possession, custody, or control. The program should cover electronic and non-electronic nonpublic information. Nonpublic information includes information that is not publicly available and covers material business information of the licensee as well as specified personal, financial and health information concerning a consumer or a family member. The Model calls for oversight by the board of directors or an appropriate board committee, the designation of a responsible person for the ISP and oversight and due diligence of all third-party service providers. A licensee must also monitor its program to adjust for changes in technology and must establish a written incident response plan. The Model includes specific requirements for investigation and notification to the commissioner in the case of a cybersecurity event. A cybersecurity event is defined as an event resulting in unauthorized access

to, disruption, or misuse of an information system or information stored on such system. It does not include encrypted information where the key has not been acquired, released or used, or events where the licensee has determined that the nonpublic information has not been used or released and has been returned or destroyed. Notification to the commissioner of the domicile or home state, and any other state where 250 or more impacted insureds reside, is required within 72 hours from determining a cybersecurity event has occurred. Notification to affected consumers is governed by the state general data breach notification laws with copies of such notices provided to the commissioner. A Licensee is required to certify to the commissioner annually (no later than February 15) that it is in compliance with the requirements of "Section 4 – Information Security Program," as well as maintain the materials and documentation used to support the certification for five years. The Model provides for three exceptions from the Section 4 ISP requirements: a licensee with fewer than 10 employees (including independent contractors), licensees who certify in writing that they have established and maintain an ISP that meets HIPAA requirements, and a licensee who is an employee, agent, representative, or designee of another licensee, but is covered by that licensee's ISP as long as that program complies with Section 4. After evolving through multiple versions and considering a multitude of comments from the insurance industry and interested parties, Version 6 of the Model significantly tracks New York's Cybersecurity Regulation (NY Regulation). Importantly, the Model includes a drafting note indicating that the Cybersecurity WG intends compliance with NY Regulation to satisfy the Model's requirements. The note states, "The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, *Cybersecurity Requirements for Financial Services Companies*, effective March 1, 2017, such Licensee is also in compliance with this Act." Examples of some major similarities with the NY Regulation include:

- Several similar definitions such as: cybersecurity event, information system, multi-factor authentication, nonpublic information, person, and publicly available information. Unlike the Model, it is important to note that the New York Regulation covers electronic information only, and, with respect to the cybersecurity event definition includes "any act or attempt, successful or unsuccessful."
- Both the Model and the NY Regulation require that the licensee perform a risk assessment.
- Written policies and procedures addressing the ISP, third-party vendor management and incident response.
- Annual reporting to the board of directors, or similar authority, by the person responsible for an ISP.
- Requirement to ensure the use of secure development practices for in-house developed applications and procedures for evaluating, assessing or testing the security of externally developed applications.

- Notification to the commissioner as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred.
- Annual documentation of compliance with the ISP.
- An exemption for licensees with fewer than 10 employees.

While many industry participants view the inclusion of the NY Regulation concepts as a positive development, there is still industry concern regarding several aspects of the Model, including its confidentiality and notice requirements. Carlton Fields Jorden Burt, P.A. will continue to monitor the Data Security Model Law's progress, including whether eventual state adoption of the Model is uniform and includes the New York safe harbor intended by the Cybersecurity WG.

Related Practices

Cybersecurity and Privacy
Financial Services Regulatory

Related Industries

Securities & Investment Companies
Life, Annuity, and Retirement Solutions