

## NAIC Exposes Second Draft of Insurance Data Security Model Law

Author:

James S. Gkonos

### SUMMARY

On August 17, 2016, the National Association of Insurance Commissioners' Cybersecurity Task Force of the Executive Committee exposed for comment the second draft of the Insurance Data Security Model Act. The second exposure draft remains true to the concepts that the NAIC adopted in its 12 core principles of regulatory guidance and Cybersecurity Bill of Rights adopted in 2015, but also makes significant changes and concessions to the insurance industry.

The first draft, which was exposed in March 2016, followed shortly after the Task Force adopted a policyholder Bill of Rights and imposed significant obligations on all licensed insurers and producers ("licensees") in the possession of personal information of applicants, insureds and their families. The first draft required significant board and C-level involvement in the risk assessment, development, implementation and review of licensees' cybersecurity plans. It also required that:

1. The cybersecurity plan conform to NIST guidelines;
2. Licensees share information through Information Sharing and Analysis Organizations ("ISAO");
3. In the event of a breach, licensees provide notice and guidance on the availability of remedies required by the Bill of Rights (including credit monitoring and notice to consumer credit reporting companies), and in some cases pay for identity theft services;
4. Licensees impose specific obligations on third-party service providers and indemnify for any data breaches;
5. Notice be provided to every insurance commissioner with affected consumers in his or her state and that such commissioners be permitted to review and edit communications with such affected policyholders;
6. Insurance commissioners have substantial enforcement powers (civil penalties and potential license revocation); and
7. Affected consumers be granted a private right of action against any licensee that violated the act.

Substantial comments were received after the first exposure and the Task Force engaged in a dialogue with the industry regarding those comments.

The second exposure draft remained true to the concepts that the NAIC adopted in its 12 core principles of regulatory guidance and Cybersecurity Bill of Rights adopted in 2015, but also made significant changes and concessions to the insurance industry. The new draft continues to impose

significant planning, implementation and updating of cybersecurity plans on boards of directors and C-level suites of larger licensees. The new draft attempts to make the responsibilities more scalable by making the responsibilities “[c]ommensurate with 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...” Section 4(A), (D)(1). It also maintains many of the requirements for notice to insureds and affected consumers and remedial obligations set out in the Bill of Rights.

However, the draft now has deleted the requirement of compliance with the NIST guidelines and sharing information with ISAOs in favor of compliance with the more amorphous “generally accepted cybersecurity principles” and now requires use of “state of the art techniques” for security. Section 4(D) (3). While licensees will continue to be required to engage only third party service providers who can maintain appropriate safeguards for personal information, the new draft deleted the list of contractual obligations imposed by the first exposure draft and limits the liability of the licensees to breaches of the personal information provided to the third party by the licensee. Licensees are still required to provide copies of notices to the insurance commissioners to ensure compliance, but the rights of the commissioners to edit such notices have been removed.

Finally, the grant of private rights of action has been deleted, and the administrative procedures and penalties for violating the act have been left to each state to determine.

A new round of comments from the insurance industry is due on September 16, 2016. Saul Ewing’s Insurance Practice will continue to monitor and report on these developments as they occur. Please direct any questions about the Model Act or this alert to the author at [jgkonos@saul.com](mailto:jgkonos@saul.com).

---

This Alert was written by James S. Gkonos, a member of the firm’s Insurance Practice. James can be reached at 215.972.8667 or [jgkonos@saul.com](mailto:jgkonos@saul.com). This publication has been prepared by the Insurance Practice for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute “Attorney Advertising.”

© 2016 Saul Ewing LLP, a Delaware Limited Liability Partnership.  
 ALL RIGHTS RESERVED.