Privacy professionals, insurance regulators, and industry insiders have been closely watching the progress of the National Association of Insurance Commissioners’ Insurance Data Security Model Law (the “Model Law”). The Model Law was formally approved in October 2017; it has recently been enacted in one state (South Carolina), and other jurisdictions have passage within their sights (Rhode Island, Vermont, Louisiana, and the District of Columbia). The NAIC is aiming for complete passage in all fifty states within the next five years. Because of the Model Law’s sweeping changes to data security and reporting, it is essential that insurers and other organizations affected by the Model Law begin preparations now to ensure timely compliance.
Every state, the District of Columbia, and Puerto Rico currently has a general data breach notification law that requires businesses to notify consumers an unauthorized individual has accessed personal information. Those notification provisions, however, vary greatly by jurisdiction — for example, if a consumer in Pennsylvania has his or her information compromised, a business must notify the consumer and, depending on the size of the breach, various consumer reporting agencies. If the same breach affects a consumer in New Jersey, however, the business would have vastly different reporting obligations, including reporting to the New Jersey Attorney General. Because data breach reporting laws apply to the residence of the consumer, not the company, it is very likely that a business may be facing a patchwork of somewhat contradictory reporting obligations in the event of a breach.

The Model Law adds yet another layer of cybersecurity regulation to the already-complex maze of best practices, industry standards, and regulatory obligations facing insurance companies today. It was heavily influenced by the groundbreaking New York State Department of Financial Services’ Cybersecurity Regulation (23 N.Y.C.R.R. 500) issued in March 2017, which applies to many financial services entities, including insurance companies, licensed in New York. Indeed, the law was so influenced by New York that it has a specific carve-out, stating that an insurer is exempt from the law if it is in compliance with New York’s cybersecurity provisions. As with all model legislation, however, this carve-out does not need to be accepted by individual state legislatures. For example, the South Carolina law does not incorporate this language, and Rhode Island’s current version of the Model Law does not contain this language. Pennsylvania may introduce its own variation of the Model Law, which may complicate compliance efforts for the insurance industry.

**To Whom Does the Model Law Apply?**

The Model Law applies to any individual or nongovernmental entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of the individual state. It does not include purchasing groups, risk retention groups chartered and licensed in another state, or any entity that is acting as an assuming insurer domiciled in another state. Those covered by the law are referred to as “licensees.”

**Although the Model Law Has Yet to Be Enacted in Pennsylvania and Licensees Will Have One Year to Comply After Enactment, Many of Its Requirements May Necessitate Comprehensive Changes to a Covered Entity’s Processes, and May Require Allocating Additional Resources to Information Management.**

Licensees with fewer than ten employees, including independent contractors, are exempt from the Model Law. Additionally, HIPAA-covered entities that maintain an information security program as defined under HIPAA are deemed to be in compliance with the Model Law information security program requirement, provided that a simple written statement of compliance is submitted to the insurance commissioner.

**What Are the Model Law’s Requirements?**

Some of the Model Law’s key requirements include:

- Licensees must maintain a written information security program, which identifies reasonably foreseeable threats to nonpublic information and the licensees’ information systems. Importantly, these also include systems that are accessible to or held by, any third-party vendors. It must also assess the likelihood of potential damage of threats and the sufficiency of policies, procedures, and information systems, that respond to those threats. This assessment must be done annually.

  - Licensees must maintain a written information security program based on the risk assessment. The information security program must include administrative, technical, and physical safeguards for the production of nonpublic information and the system itself.

- Risk management must be given priority. Any information security program must be designed to mitigate key risk, and third-party service providers are required to be included in the program. Key security measures to be implemented include access controls, physical security, data encryption while in transit and while at rest on storage devices/laptops, secure development practices for in-house applications, multifactor authentication, testing and monitoring of systems and procedures, audit trails, disaster recovery in the event of a catastrophic or technological failure, and secure disposal.

- Cybersecurity awareness training is required for personnel and, again, is informed by risks identified in the risk assessment.

- There must be significant board involvement in the cybersecurity process if the licensee has a board of directors. The law specifically requires the board, or an appropriate committee of the board, to create an information security program.
and receive a written report regarding key cybersecurity matters annually.

- **Third-party service provider oversight** is a must. Vendors that come into contact with nonpublic information or the network should be chosen closely and selectively. Licensees must require third-party service providers to implement appropriate administrative, technical and physical measures to secure information systems and the public information. This may require rewriting contracts for third-party service providers.

- All licensees must have an **incident response plan** designed to respond to and recover from any cybersecurity event promptly. The Model Law enumerates various requirements of the incident response plan.

- Each insurer is required to submit written certification of compliance to its Insurance Commissioner annually.

- Investigations surrounding cybersecurity events must be done promptly. At a minimum, the investigation by a licensee must determine:

1. Whether a cybersecurity event has actually occurred;
2. The nature and scope of the event;
3. What nonpublic information may have been involved;
4. What reasonable measures must be taken to restore the security of the compromised systems.

- A licensee must **notify the Insurance Commissioner within 72 hours** after determining that a cybersecurity event has occurred. A licensee must still provide notice to consumers under the state’s data breach notification statute, but the licensee must also provide a copy of the notice sent to consumers to the Commissioner.

**What Should Be the First Step?**

Although the Model Law has yet to be enacted in Pennsylvania and licensees will have one year to comply after enactment, many of its requirements may necessitate comprehensive changes to a covered entity’s processes, and may require allocating additional resources to information management. Consider taking first steps now, such as hiring a third party to perform a comprehensive risk assessment, reviewing internal security policies and procedures, reassessing budgets, and reexamining third party vendor agreements, to ensure that they are in line with the Model Law. Although the exact language of the Model Law as it is enacted in Pennsylvania may change some of these requirements, many of its underlying principles constitute best practices for organizations operating in the insurance space.

Jana Landon, CIPP/US, is Co-Chair of the Cyber Insurance and Data Breach Teams at Stradley Ronon Stevens & Young, LLP. Her practice focuses on advising clients on data security and data management issues and strategic issues regarding information governance. She also acts as a data breach coach.