OLR Bill Analysis
SB 903

AN ACT CONCERNING INSURANCE DATA AND INFORMATION SECURITY.

SUMMARY

This bill repeals the state’s information security program law, replacing it with provisions substantially similar to the National Association of Insurance Commissioners (NAIC) insurance data security model law.

Current law requires insurers, pharmacy benefit managers (PBMs), third-party administrators (TPAs), utilization review companies, and any other entity licensed to do health insurance business to implement and maintain a written comprehensive information security program to safeguard the personal information of insureds and enrollees. Among other things, the program must be appropriate to the business’ size, scope, type, available resources, and data, and the type of security and confidentiality necessary.

The bill generally incorporates current law’s information security provisions as they relate to data security breaches, access control measures, investigations, reporting, and oversight. However, the bill’s requirements are more comprehensive and apply to all entities licensed under the insurance statutes, excluding a purchasing or risk retention group chartered in another state and nondomiciled assuming insurers. The bill also protects consumers’ “nonpublic information,” not just personal information under current law. Specifically the bill:

1. requires licensees to develop a risk assessment program, investigate cybersecurity events, and notify the insurance commissioner of any such event within 72 hours;

2. authorizes the commissioner to enforce its provisions; fine violators up to $50,000; and adopt implementing regulations;
and

3. applies existing law’s identity theft mitigation and data breach security requirements to all licensees as it related to the breach of consumers’ nonpublic information.

The bill defines “nonpublic information” as information that is not public, not related to age or gender, and that (1) would materially impact a licensee’s business, operation, or security if disclosure, (2) is created or derived from a consumer or health care provider and concerns behavioral, mental, or physical health or health care services or payments, or (3) concerns a consumer’s name, number, or other personal identifiable information that can identify a consumer when used in combination with an access or security code; account, credit or debit card number; biometric records; driver’s license or identification number; or Social Security number.

Under the bill, a “cybersecurity event” is unauthorized access to information systems or nonpublic information.

EFFECTIVE DATE: October 1, 2019, for the provisions related to the new Insurance Data Security Law (§ 1); October 1, 2020, for the provisions related to existing identity theft mitigation services requirements (§ 2); and October 1, 2020, for the repeal of the current Comprehensive Information Security Program law (§ 3).

§ 1 — NEW INSURANCE DATA SECURITY LAW

The bill requires licensees to:

1. develop and implement risk assessment and information security programs to protect nonpublic information; and

2. along with certain third-party service providers (i.e., entities that can access or are contracted with a licensee to maintain, process, or store nonpublic information) investigate cybersecurity events and, within 72 hours, report any such event to the commissioner.

(These provisions are effective October 1, 2019, and require
implementation of the risk assessment program by July 1, 2020. The bill repeals and replaces the current information security program requirements on October 1, 2020, thus resulting in a three-month period during which both sets of program requirements apply.)

**Risk Assessment Program**

Program Requirements. The bill requires each licensee to implement a continuously operated risk assessment program by July 1, 2020, that:

1. designates an affiliate, employee, or outside vendor to develop, implement, and maintain an information security program;

2. identifies reasonably foreseeable internal and external threats (a) that might result in unauthorized access or alteration, destruction, disclosure, misuse, or transmission of nonpublic information held by the licensee or (b) to the licensee’s security information systems and nonpublic information in possession, custody, or control of, or accessible to, a third-party service provider;

3. assesses the likelihood and potential damage of reasonably foreseeable threats, taking into account the sensitivity of any nonpublic information; and

4. implements information safeguards, including key controls, procedures, and systems, to manage reasonably foreseeable threats and assess them at least annually.

The risk assessment program must also assess the sufficiency of the licensee’s information system and all policies, procedures, and safeguards to manage against reasonably foreseeable threats that might originate from the licensee’s operation (e.g., internal threats). This assessment must include (1) employee training and management; (2) information systems, including network and software design, and information classification, disposal, governance, processing, storage, and transmission; and (3) detection, prevention, and response to cyber security events.
**Post-Implementation.** The bill also requires each licensee, on the basis of the risk assessment program, to:

1. include cybersecurity risks in their enterprise risk management process;
2. remain informed of emerging threats and vulnerabilities;
3. utilize reasonable security measures relative to the data’s type and sensitivity when sharing it; and
4. provide employees with up-to-date and ongoing cybersecurity awareness training that accounts for all risks the assessment program identifies.

**Security Measures.** Licensees must also determine and implement the following security measures, as appropriate:

1. access control measures for information systems, including ways to identify and restrict access to authorized individuals;
2. measures that identify and manage data, device, facilities, personnel, and systems as appropriate to the licensee’s business;
3. measures that restrict access to physical locations containing nonpublic information to authorized individuals;
4. measures that protect, by encryption or other means, nonpublic information while it is being transmitted over an external network or stored on a laptop or other portable device;
5. secures development measures for software applications the licensee develops and uses;
6. measures for assessing, evaluating, and testing the security of software applications the licensee uses that were developed by someone else;
7. measures to modify the licensee’s information systems in accordance with its information security program (see below);
8. effective control measures, including multifactor authentication for individuals accessing nonpublic information;

9. measures to include audit trails within the information security program to detect and respond to cybersecurity events and reconstruct material financial transactions;

10. measures to regularly rest and monitor the information systems and procedures to detect both actual and attempted attacks;

11. measures to protect against damage or destruction, or loss of nonpublic information caused by environmental hazards, including fire, water, catastrophes, or technological failures; and

12. measures to dispose of nonpublic information regardless of its format.

Information Security Program

Plan Design. The bill requires licensees, by October 1, 2020, to develop, implement, and maintain an information security program based on the risk assessment program described above that:

1. is commensurate with the (a) licensee’s complexity, size, nature, and business scope, including any use of third-party service providers and (b) sensitivity of the nonpublic data used by, or in possession or control of, the licensees information systems; and

2. establishes and provides for periodic reevaluation of a nonpublic data retention schedule and a mechanism for destroying it once the licensee is done using the data.

The plan must be designed to:

1. protect against hazards or threats to the (a) integrity and security of the licensee’s information systems and (b) confidentiality and security of nonpublic information held or controlled by the licensee and

2. minimize the likelihood of harm to consumers resulting from
any unauthorized access to, or use of, nonpublic information.

**Written Incident Response Plan.** The plan must also include a written incident response plan that:

1. is designed to promptly respond to, and recover from, cybersecurity events that compromise a licensee’s information systems, business operations, or the confidentiality, availability, or integrity of nonpublic information it holds;

2. addresses the licensee’s internal response process to cybersecurity events, including clearly defining the responsibilities, roles, and levels of decision making authority;

3. establishes goals for the plan;

4. addresses both internal and external communications and information sharing;

5. identifies requirements for remediating any weakness in the licensee’s information systems or controls;

6. provides for the documenting and reporting of cybersecurity events and response activities; and

7. establishes a process to evaluate and if necessary revise the plan.

**Plan Evaluation.** Under the bill, each licensee must evaluate, monitor, and adjust the information security program consistent with:

1. relevant technological changes;

2. the sensitivity of the nonpublic information;

3. threats to nonpublic information, regardless of where they originate;

4. changes in a licensee’s business arrangements, including acquisitions, alliances, joint ventures, mergers, and outsources; and
5. changes in licensee information systems.

**Board of Directors Requirements.** If a licensee is governed by a board of directors, the board or one of its committees must require the licensee’s executive management or a designee to develop, implement, and maintain the information security program and report at least annually to the board about the program’s status and related matters. This must include control decisions, cybersecurity events and responses, recommended changes, the ongoing risk assessment, testing results, and any arrangements with third-party providers.

If the executive management designates an individual who is not in an executive management role to perform these responsibilities, the bill requires the executive management to oversee the development, implementation, and maintenance of the program and require that the designee report to it with the same information described above that must be reported to the board.

**Third Party Service Provider Contracts**

By October 1, 2021, the bill requires licensees that contract with third-party service providers or allow them access to their nonpublic information to implement appropriate administrative, physical, and technical measures to protect and secure all nonpublic information that they hold or to which they have access. Under the bill, each licensee must exercise due diligence in selecting third-party service providers.

**Certification to Commissioner and Record Retention Requirements**

Annually, starting by February 15, 2021, the bill requires domestic insurers to submit to the insurance commissioner, in a form and manner he prescribes, a written statement certifying that the insurer has complied with the bill’s risk assessment and information security program provision. Each domestic insurer must maintain all supporting documents, including data, information, records, and schedules, for at least five years after submitting its certification.

The bill also requires a domestic insurer that identifies areas, process, or systems that require material improvements, redesigns, or
updates to document and identify the remediation efforts planned and underway and make such documents available to the commissioner on request.

Beginning October 1, 2020, the bill requires each licensee to retain records of cybersecurity events for at least five years after the event occurs.

**72-Hour Reporting Requirement**

The bill establishes notification requirements for licensees and third-party service providers following cybersecurity events.

**Licensees.** Under the bill, each licensee must notify the commissioner, in a form and manner he prescribes, within 72 hours of a cybersecurity event if the licensee:

1. is an insurer domiciled in the state (i.e., a domestic insurer) or an insurance producer whose home state is Connecticut or

2. reasonably believes the nonpublic information involved in the cybersecurity event effects 250 people or more and (a) the licensee is required to send a cybersecurity notice to any governing, regulatory, or supervisory body under federal or state law or (b) it is reasonably likely the cybersecurity event will materially harm any consumer or the licensee’s business.

If a licensee is acting as an assuming insurer (i.e., an insurer that acquires an insurance obligation from another insurer), it must notify the commissioner and the ceding insurer (i.e., the insurer that transferred the obligations) within 72 hours if the cybersecurity event involves nonpublic information that is (1) possessed, controlled, or involves information systems maintained by the licensee in its capacity as an assuming insurer or (2) stored on the information systems of a third-party service provider that contracts with the licensee in its capacity as an assuming insurer.

**Third-Party Service Providers.** Under the bill, on and after October 1, 2020, a third-party service provider that discovers a
cybersecurity event on its own systems must notify, within 72 hours, each licensee it contracts with and that is affected by the event. The notification must be in a form and manner prescribed by the commissioner.

**Notice to Commissioner**

Any insurer that receives notice of a cybersecurity event from a third-party service provider or is required under the bill to notify the commissioner of an event must, in an electronic form prescribed by the commissioner, submit the following information and update it as new information becomes available:

1. the date the cybersecurity event occurred, how it was discovered, and the perpetrator’s identity;

2. a description of how nonpublic information was breached, exposed, lost, or stolen, including the specific responsibilities and roles of any third-party service provider involved;

3. how much, if any, nonpublic information was recovered and how, and a description of the specific type of nonpublic information, including whether it was financial or medical information;

4. whether the licensee notified any government, law enforcement, or regulatory agency other than the insurance commissioner, and if so, when;

5. the period during which the information system was compromised and the number of consumers affected by the cybersecurity event, or the licensee’s best estimate if the number is unavailable;

6. the results of any review the licensee conducted that (a) identifies lapses in automated controls or internal procedures or (b) confirms that all controls and procedures were followed;

7. a description of any efforts undertaken to remediate the
conditions that caused the event and a copy of any privacy policy the licensee implemented or used;

8. a statement outlining all the steps the licensee will take to (a) investigate the event and (b) notify affected consumers;

9. the name of an individual familiar with the event and authorized to act on the licensee’s behalf; and

10. a copy of any required notice to impacted consumers (see below).

**Notice to Consumers**

The bill requires (1) any insurer that notifies the commissioner of a cybersecurity event and (2) any ceding insurer who receives notice from an assuming insurer of an event and maintains a contractual relationship with impacted consumers to notify consumers within 90 days as required under existing law (CGS § 36a-701b).

If a consumer accessed affected services through an insurance producer, and the licensee has the producer’s current contact information, the licensee must notify the producer of the event in a form and manner the commissioner prescribes.

**Cybersecurity Event Investigations**

The bill requires licensees that suspect a cybersecurity event involving its systems to promptly investigate and, at a minimum, determine whether the event occurred. If the licensee determines that the event occurred, it must:

1. assess the event’s nature and scope;

2. identify all nonpublic information that might have been involved; and

3. perform, or oversee implementing, reasonable procedures to restore system security and prevent further unauthorized acquisition, release, or use of nonpublic information.
If a licensee is notified by a third-party service provider of a cybersecurity event or otherwise has knowledge such an event has occurred, it must (1) immediately conduct an investigation as described above or (2) confirm, that the third-party service provider has conducted such an investigation and maintain records of such confirmation.

**Enforcement**

Beginning October 1, 2020, the bill requires the commissioner to enforce the bill’s cybersecurity provisions and authorizes him to do so in accordance with his existing powers. It also requires him to issue and serve the licensee with a statement of the violation and notice of a hearing, to be held at least 30 days after the notice is served.

The licensee must have an opportunity to be heard and show cause why an order should not be entered by the commissioner enforcing the bill’s provisions or suspending, revoking, or refusing to reissue or renew any license, registration, or authorization issued by the commissioner.

The commissioner may, after a hearing and in addition to or in lieu of actions he takes against the licensee’s license, registration, or authorization, impose a civil penalty up to $50,000 for each violation. Under the bill, the commissioner may bring a civil action to recover any penalty imposed.

The bill allows the commissioner to exercise his authority in any legal or regulatory action using any documents, information, and material submitted to, or obtained during an investigation by, the commissioner.

**Confidentiality**

The bill makes all documents submitted to or obtained by the commissioner during an investigation confidential and privileged. They are exempt from disclosure under the state’s Freedom of Information Act (FOIA) and any subpoena or discovery in a private cause of action. The bill also prohibits such documents from being
introduced as evidence in a private cause of action. It prohibits the commissioner and all persons acting on his behalf who receive confidential information from being allowed or compelled to testify in a private cause of action that concerns the confidential material.

He may submit such documents, information, and material to the (1) Attorney General or another state, federal, or international regulatory or law enforcement agency and (2) NAIC and its affiliates and subsidiaries, provided they agree in writing to maintain the same level of confidentiality. He may also (1) receive documents and information from these sources, provided he treats them as confidential, and (2) submit documents and information to third-party consultants or vendors, provided they agree in writing to maintain the documents’ and information’s confidentiality.

The commissioner may enter agreements governing the submission of documents, information, and materials in a way that maintains confidentiality.

Regardless of the bill’s other provisions, it authorizes him to release to any NAIC clearinghouse or database a final adjudicated action that is subject to disclosure under FOIA.

The bill specifies that no waiver of any applicable privilege or claim of confidentiality in any document, information, or material occurs as a result of submitting it to, or it being received by, the commissioner.

**Exemptions**

The bill exempts independent contractors and licensees with nine or fewer employers from the risk assessment and information security program provisions, but still (1) requires them to report cybersecurity events under the bill’s provisions and (2) extends the commissioner’s enforcement authority over them.

Licensees subject to the federal Health Insurance Portability and Accountability Act that establish and maintain an information security program under the act are deemed to have satisfied the bill’s risk assessment and information security program provisions. In such a
In this case, the licensee must certify to the commissioner, in a form and manner he prescribes, that it complies with the federal law.

The bill also specifies that its provisions apply to licensees, and not their agents, designees, employees, or representatives, provided they are covered by the licensee’s information security program. Licensees that cease to meet this exemption must comply with the bill’s provisions within 180 days.

**Private Right of Action**

The bill specifies that it must not be construed to create a private right of action, or to affect or limit an existing private right of action.

**§ 2 — EXISTING IDENTITY THEFT MITIGATION AND DATA BREACH SECURITY LAW**

The bill adds “nonpublic information” to the state’s data breach privacy laws. In doing so, starting October 1, 2020, it requires any person or business that owns or licenses computerized data that includes personal information to notify consumers if any of their nonpublic information has been breached or reasonably believed to have been breached and provide them up to two years of identity theft mitigation services, as is required under existing law regarding consumers’ personal information. By law, personal information is an individual’s first name or initial and last name with his or her (1) Social Security, driver’s license, state identification number; (2) credit or debit card number; or (3) financial account number in combination with a password that allows access to the account (CGS § 36a-701b).

**COMMITTEE ACTION**

Insurance and Real Estate Committee

Joint Favorable

Yea 19  Nay 0  (03/14/2019)