2019 SESSION

19-0923
01/04

SENATE BILL ***194-FN***

AN ACT relative to the insurance data security law.

SPONSORS: Sen. Morgan, Dist 23; Sen. Feltes, Dist 15; Sen. Soucy, Dist 18; Rep. Hunt, Ches. 11

COMMITTEE: Commerce

ANALYSIS

This bill establishes the insurance data security law.

This bill is a request of the insurance department.

- -

Explanation: Matter added to current law appears in ***bold italics.***
Matter removed from current law appears [~~in brackets and struckthrough.~~]
Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.
19-0923
01/04

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Nineteen

AN ACT relative to the insurance data security law.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 New Chapter; Insurance Data Security Law. Amend RSA by inserting after chapter 420-O the following new chapter:

CHAPTER 420-P

INSURANCE DATA SECURITY LAW

420-P:1 Title. This chapter shall be known and may be cited as the "Insurance Data Security Law."

420-P:2 Purpose and Scope.

I. This chapter establishes the exclusive state standards applicable to licensees for data security, the investigation of a cybersecurity event, as defined in RSA 420-P:3, IV, and notification to the commissioner.

II. This chapter shall not be construed to create or imply a private cause of action for violation of its provisions nor shall it be construed to curtail a private cause of action which would otherwise exist in the absence of this chapter.

420-P:3 Definitions. In this chapter:

I. “Authorized individual” means an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems.

II. “Commissioner” means the insurance commissioner.

III. “Consumer” means an individual, including, but not limited to, applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control.

IV. “Cybersecurity event” means an event resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic information stored on such information system. The term shall not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization. A cybersecurity event shall not include an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

V. “Department” means the insurance department.

VI. “Encrypted” means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

VII. “Information security program" means the administrative, technical, and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.

VIII. “Information system” means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic nonpublic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

IX. “Licensee” means any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

X. “Multi-factor authentication” means authentication through verification of at least 2 of the following types of authentication factors:

(a) Knowledge factors, such as a password;

(b) Possession factors, such as a token or text message on a mobile phone; or

(c) Inherence factors, such as a biometric characteristic.

XI. “Nonpublic information” means information that is not publicly available information and is:

(a) Any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify such consumer, in combination with any one or more of the following data elements:

(1) Social Security number.

(2) Driver’s license number or non-driver identification card number.

(3) Financial account number, credit or debit card number.

(4) Any security code, access code or password that would permit access to a consumer’s financial account.

(5) Biometric records.

(b) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer, that can be used to identify a particular consumer, and that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of any consumer or a member of the consumer's family;

(2) The provision of health care to any consumer; or

(3) Payment for the provision of health care to any consumer.

XII. "Person" means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency, or association.

XIII. "Program" means information security program.

XIV. "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law. For the purposes of this paragraph, a licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.

XV. "Risk assessment" means the risk assessment that each licensee is required to conduct under RSA 420-P:4, III.

XVI. "State" means the state of New Hampshire.

XVII. "Third-party service provider" means a person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

420-P:4 Information Security Program.

I. Implementation of the program shall be commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

II. The objectives of a licensee's program shall be designed to:

(a) Protect the security and confidentiality of nonpublic information and the security of the information system.

(b) Protect against any threats or hazards to the security or integrity of nonpublic information and the information system.

(c) Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer.

(d) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

III. While performing risk assessment the licensee shall:

(a) Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee who is responsible for the program.

(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

(c) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information.

(d) Assess the sufficiency of policies, procedures, information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and

(3) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

(e) Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

IV. Based on its risk assessment and to manage its risk, the licensee shall:

(a) Design its program to mitigate the identified risks, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control.

(b) Determine which security measures listed below are appropriate and implement such security measures:

(1) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information.

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy.

(3) Restrict physical access to nonpublic information to authorized individuals only.

(4) Protect by encryption or other appropriate means, all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media.

(5) Adopt secure development practices for in-house developed applications utilized by the licensee.

(6) Modify the information system in accordance with the licensee's information security program.

(7) Utilize effective controls, which may include multi-factor authentication procedures for any individual accessing nonpublic information.

(8) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

(9) Include audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee.

(10) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures.

(11) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

(c) Include cybersecurity risks in the licensee's enterprise risk management process.

(d) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(e) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

V. If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(a) Require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program.

(b) Require the licensee's executive management or its delegates to report in writing at least annually, the following information:

(1) The overall status of the information security program and the licensee's compliance with this chapter; and

(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the program.

(c) If executive management delegates any of its responsibilities under RSA 420-P:4, it shall oversee the development, implementation and maintenance of the licensee's program prepared by the delegates and shall receive a report from the delegates complying with the requirements of the report to the board of directors.

VI.(a) With regard to oversight of third-party service providers, a licensee shall exercise due diligence in selecting its third-party service provider; and

(b) A licensee shall require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

VII. The licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

VIII.(a) As part of its program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations.

(b) Such incident response plan shall address the following areas:

(1) The internal process for responding to a cybersecurity event;

(2) The goals of the incident response plan;

(3) The definition of clear roles, responsibilities, and levels of decision-making authority;

(4) External and internal communications and information sharing;

(5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(6) Documentation and reporting regarding cybersecurity events and related incident response activities; and

(7) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

IX. Annually, each insurer domiciled in this state shall submit to the commissioner, a written statement by March 1, certifying that the insurer is in compliance with the requirements set forth in this section. Each insurer shall

maintain for examination by the department all records, schedules and data supporting this certificate for a period of 5 years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation shall be available for inspection by the commissioner.

420-P:5 Investigation of a Cybersecurity Event.

I. If the licensee learns that a cybersecurity event has or may have occurred, the licensee or an outside vendor and/or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.

II. During the investigation, the licensee, or an outside vendor and/or service provider designated to act on behalf of the licensee, shall, at a minimum determine as much of the following information as possible:

(a) Whether a cybersecurity event has occurred.

(b) The nature and scope of the cybersecurity event.

(c) Identify any nonpublic information that may have been involved in the cybersecurity event.

(d) Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release or use of nonpublic information in the licensee's possession, custody or control.

III. If the licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee shall complete the steps listed in paragraph II above or confirm and document that the third-party service provider has completed those steps.

IV. The licensee shall maintain records concerning all cybersecurity events for a period of at least 5 years from the date of the cybersecurity event and shall produce those records upon demand of the commissioner.

420-P:6 Notification of a Cybersecurity Event.

I. Each licensee shall notify the commissioner within 3 business days of a determination that a cybersecurity event has occurred when either of the following criteria has been met:

(a) New Hampshire is the licensee's state of domicile, in the case of an insurer, or this state is the licensee's home state, in the case of a producer, as those terms are defined in RSA 402-J, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or reasonable likelihood of materially harming any material part of the normal operations of the licensee; or

(b) The licensee reasonably believes that the nonpublic information involves 250 or more consumers residing in New Hampshire and that the cybersecurity event:

(1) Impacts the licensee, in which case notice shall be provided to any government body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law; or

(2) Has a reasonable likelihood of materially harming:

(A) Any consumer residing in this state; or

(B) Any material part of the normal operations of the licensee.

II. The licensee shall provide as much of the following information as possible. The licensee shall provide the information in electronic form as directed by the commissioner. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner regarding material changes to previously provided information relating to the cybersecurity event.

(a) Date of the cybersecurity event.

(b) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.

(c) How the cybersecurity event was discovered.

(d) Whether any lost, stolen, or breached information has been recovered and, if so, how this was done.

(e) The identity of the source of the cybersecurity event.

(f) Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.

(g) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.

(h) The period during which the information system was compromised by the cybersecurity event.

(i) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section.

(j) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.

(k) Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.

(l) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.

(m) Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

III. As to notification to consumers, a licensee shall comply with RSA 359-C:20, I(a) and (c), II-IV, and VI, and provide a copy of the notice sent to consumers under that statute to the commissioner, when a licensee is required to notify the commissioner under paragraph I.

IV.(a) In the case of a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat such event as it would under paragraph I, unless the third-party service provider provides the notice required under paragraph I to the commissioner.

(b) The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

(c) Nothing in this chapter shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider or any other party to fulfill any of the investigation requirements imposed under RSA 420-P:5 or notice requirements imposed under RSA 420-P:6.

V.(a)(1) As to notice of cybersecurity events of reinsurers to insurers, in the case of a cybersecurity event involving nonpublic information that is used by the licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within 3 business days of making the determination that a cybersecurity event has occurred.

(2) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under RSA 359-C:20, I (a) and (c), II-IV, and VI, and any other notification requirements relating to a cybersecurity event imposed under this section.

(b)(1) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within 3 business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(2) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under RSA 359-C:20, I (a) and (c), II-IV, and VI, and any other notification requirements relating to a cybersecurity event imposed under this section.

(c) Any licensee acting as assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

VI. As to notice of cybersecurity events from insurers to producers of record, in the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a licensee that is an insurer or its third-party service provider and for which a consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected consumers as soon as practicable as directed by the commissioner. The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual consumer.

420-P:7 Power of Commissioner.

I. The commissioner shall have power to examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this chapter. This power is in addition to the powers which the commissioner has under RSA 400-A:16 and RSA 400-A:37. Any such investigation shall be conducted pursuant to RSA 400-A:16 and any examination shall be conducted pursuant to 400-A:37.

II. Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state which violates this chapter, the commissioner may take action that is necessary or appropriate to enforce the provisions of this chapter.

420-P:8 Confidentiality.

I. Any documents, materials, or other information in the control or possession of the department that are furnished by a licensee or an employee or agent thereof acting on behalf of licensee pursuant to RSA 420-P:4, IX, RSA 420-P:6, II(b), (c), (d), (e), (h), (j), and (k), or that are obtained by the commissioner in an investigation or examination pursuant to RSA 420-P:7 shall be confidential by law and privileged, shall not be subject to RSA 91-A, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the commissioner may use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the commissioner's duties. The commissioner shall not otherwise make the documents, materials, or other information public without the prior written consent of the licensee.

II. Neither the commissioner nor any person who received documents, materials, or other information while acting under the authority of the commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to this section.

III. In order to assist in the performance of the commissioner's duties under this chapter, the commissioner:

(a) May share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to paragraph I, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(b) May receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information.

(c) May share documents, materials, or other information subject to paragraph I, above, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(d) May enter into agreements governing sharing and use of information consistent with this section.

IV. Nothing in this chapter shall prohibit the commissioner from releasing final, adjudicated actions that are open to public inspection, pursuant to RSA 91-A, to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

V. Documents, materials, or other information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant or vendor pursuant to this chapter shall be confidential by law and privileged, shall not be subject to RSA 91-A, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action.

VI. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in paragraph III.

420-P:9 Exceptions.

I. The following exceptions shall apply to this chapter:

(a) A licensee with fewer than 10 employees, including any independent contractors, shall be exempt from RSA 420-P:4.

(b) An employee, agent, representative, or designee of a licensee, who is also a licensee, shall be exempt from RSA 420-P:4 and need not develop its own program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(c) A continuing care retirement community, as defined by RSA 420-D, shall be exempt from RSA 420-P:4.

(d) A life settlement provider, as defined by RSA 408-D, shall be exempt from RSA 420-P:4.

II. A licensee which ceases to qualify for an exception under this section shall have 180 days to comply with RSA 420-P:4.

420-P:10 Safe Harbor for HIPAA Compliance. A licensee that is in possession of protected health information subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and that has established and maintains programs and procedures regarding information privacy, security, and breach notification that are prescribed by HIPAA and by Parts 160 and 164 of Title 45 of the Code of Federal Regulations established pursuant to

HIPAA, shall be considered to meet the requirements of this chapter with respect to such protected health information, provided that the licensee is compliant with the HIPAA privacy, security, and breach notification requirements and submits a written statement certifying such compliance. For purposes of this section, the definition of "protected health information" shall be as set forth in HIPAA and the regulations promulgated thereunder and shall be considered to be a subset of nonpublic information, as defined in RSA 420-P:3, XI.

420-P:11 Penalties. A licensee which violates this chapter may be penalized in accordance with RSA 400-A:15, III.

420-P:12 Rulemaking. The commissioner may adopt rules pursuant to RSA 541-A as necessary to carry out the provisions of this chapter.

420-P:13 Severability. If any provision of this chapter, or the application thereof to any person or circumstance is held invalid, such invalidity shall not affect other provisions or applications of this chapter which can be given effect without the invalid provision or application, and to this end the provisions of the chapter are declared to be severable.

2 Implementation by Licensees. Licensees shall have one year from the effective date of this act to implement RSA 420-P:4, I-V and VII-IX. Licensees shall have 2 years from the effective date of this act to implement RSA 420-P:4, VI.

3 Effective Date. This act shall take effect January 1, 2020.

LBAO
19-0923
1/17/19

SB 194-FN- FISCAL NOTE
AS INTRODUCED

AN ACT relative to the insurance data security law.

FISCAL IMPACT: **[X] State** **[ ] County** **[ ] Local** **[ ] None**

	Estimated Increase / (Decrease)			
STATE:	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**
Appropriation	$0	$0	$0	$0
Revenue	Indeterminable Increase	Indeterminable Increase	Indeterminable Increase	Indeterminable Increase
Expenditures	Indeterminable Increase	Indeterminable Increase	Indeterminable Increase	Indeterminable Increase
Funding Source:	[X] General [ ] Education [ ] Highway [X] Other - Insurance Assessments / Fines			

METHODOLOGY:

The Insurance Department indicates this bill proposes to adopt: the Model Law of the National Association of Insurance Commissioners in order to update and establish standards for protection of consumers' non public information; requirements for investigation of a breach; and notification to the Commissioner and consumers in the event of cyber security breaches relating to consumers' nonpublic information. The Department assumes there may be a fiscal impact depending on the compliance of the Department's licensees. Any additional expense

would be part of the Department's operating costs. Any revenue obtained through enforcement of the law, such as regulatory fines, would be deposited in the general fund. The Department is not able to accurately determine the fiscal impact of the bill at this time.

AGENCIES CONTACTED:

Insurance Department