THE SENATE
THIRTY-FIRST LEGISLATURE, 2021
STATE OF HAWAII

S.B. NO. 1100 S.D. 1 H.D. 1

A BILL FOR AN ACT

RELATING TO INSURANCE DATA SECURITY.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. The legislature finds that the National Association of Insurance Commissioners adopted the Insurance Data Security Model Law in 2017 to strengthen existing data privacy and consumer breach notification obligations of insurance licensees. The National Association of Insurance Commissioners strongly encourages that states adopt this model law by 2022, to avoid risking federal preemption of state laws in this area. While some licensees may already have cybersecurity policies and protocols in place, this Act will ensure and formalize insurance data security protections for all insurance licensees.

The purpose of this Act is to adopt the National Association of Insurance Commissioners Insurance Data Security Model Law to establish exclusive state standards applicable to insurance data security standards for Hawaii insurance licensees.

SECTION 2. Chapter 431, Hawaii Revised Statutes, is amended by adding a new article to be appropriately designated and to read as follows:

"ARTICLE

INSURANCE DATA SECURITY LAW

PART I. GENERAL PROVISIONS

§431: -101 Definitions. As used in this article:

"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.

"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.

"Cybersecurity event" means an event resulting in unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on that information system. "Cybersecurity event" does not include:

(1) The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization; and

(2) An event in 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.

"Encrypted" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

"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.

"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 systems, such as industrial controls systems, process controls

systems, telephone switching and private branch exchange systems, and environmental control systems.

"Licensee" means every licensed insurer, producer, and any other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered, under chapter 431 or 432, or holding a certificate of authority under chapter 432D. "Licensee" does not include a purchasing group or risk retention group chartered and licensed in a state other than this State, or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

"Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;

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

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

"Nonpublic information" means electronic information that is not publicly available information and is:

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

(A) Social security number;

(B) Driver's license number or non-driver identification card number;

(C) Financial account number or credit or debit card number;

(D) Any security code, access code, or password that would permit access to a consumer's financial account; or

(E) Biometric records; or

(2) Any information or data subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, except age or gender, in any form or medium created by or derived from a health care provider or a consumer that identifies a particular consumer and that relates to:

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

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

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

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

"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 purposes of this definition, 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:

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

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

"Risk assessment" means the risk assessment that each licensee is required to conduct under section 431: -202.

"State" means the State of Hawaii.

"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.

§431: -102 Powers of the commissioner. (a) The licensee's regulator 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 article.

(b) Any examination or investigation of a licensee domiciled in the State shall be conducted pursuant to section 431:2-301.7.

(c) Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in the State that

violates this article, the commissioner may take action that is necessary or appropriate to enforce the provisions of this article.

§431: -103 Confidentiality. (a) Any documents, materials, or other information in the control or possession of the commissioner that is furnished by a licensee, or an employee or agent thereof acting on behalf of the licensee pursuant to sections 431: -208 and 431: -302, or that are obtained by the commissioner in an examination or investigation pursuant to section 431: -102, shall be confidential by law and privileged, shall not be subject to chapter 92F, shall not be subject to subpoena, and shall not be subject to discovery or admissible as evidence in any private civil action. However, the commissioner may use the documents, materials, or other information obtained in an examination or investigation in the furtherance of any regulatory or legal action brought as a part of the commissioner's duties.

(b) Neither the commissioner nor any person acting under the direction of the commissioner shall be allowed or required to testify in any private civil action concerning any

confidential documents, materials, or information subject to subsection (a).

(c) To assist in the performance of the commissioner's duties under this article, the commissioner may:

(1) Share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection (a), 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;

(2) 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; provided that the commissioner 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;

(3) Share documents, materials, or other information subject to subsection (a) with a third-party consultant or vendor; provided that the consultant or vendor agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information; and

(4) Enter into agreements governing sharing and use of information consistent with this subsection.

(d) 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 subsection (c).

(e) Nothing in this article shall prohibit the commissioner from releasing final, adjudicated actions that are

open to public inspection pursuant to chapter 92F to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

§431: -104 Exceptions. (a) The following exceptions shall apply to this article:

(1) A licensee with fewer than ten employees, including any independent contractors, shall be exempt from part II;

(2) A licensee subject to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, that has established and maintains an information security program pursuant to the statutes, rules, regulations, procedures, or guidelines established thereunder shall be considered to have met the requirements of part II of this article; provided that the licensee is compliant with and submits a written statement certifying its compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; and

(3) An employee, agent, representative, or designee of a licensee, who is also a licensee, shall be exempt from part II of this article and shall not be required to develop its own information security program; provided that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(b) In the event that a licensee ceases to qualify for an exception pursuant to this section, the licensee shall have one hundred eighty days to comply with this article.

§431: -105 Penalties. In the case of a violation of this article, a licensee may be penalized in accordance with section 431:2-203.

§431: -106 Private cause of action. This article shall not be construed to create or imply a private cause of action for any violation of its provisions, and it shall not be construed to curtail a private cause of action that would otherwise exist in the absence of this article.

§431: -107 Rules. The commissioner may adopt rules pursuant to chapter 91 as necessary to carry out the provisions of this article.

PART II. INFORMATION SECURITY PROGRAM

§431: -201 Implementation of an information security program. 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.

§431: -202 Objectives of the information security program; risk assessment. (a) A licensee's information security program shall be designed to:

(1) Protect the security and confidentiality of nonpublic information and the security of the information system;

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

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

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

(b) Regarding risk assessment, the licensee shall:

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

(2) 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;

(3) Assess the likelihood and potential damage of the reasonably foreseeable internal or external threats,

taking into consideration the sensitivity of the nonpublic information;

(4) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage the reasonably foreseeable internal or external threats, including consideration of threats in each relevant area of the licensee's operations, including:

(A) Employee training and management;

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

(C) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) 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.

§431: -203 Risk management. Based on its risk assessment, the licensee shall:

(1) Design its information security program to mitigate the identified risks, commensurate with the size and complexity 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;

(2) Determine which security measures listed in this paragraph are appropriate and implement those security measures:

(A) 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;

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

(C) Restrict access at physical locations containing nonpublic information only to authorized individuals;

(D) 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;

(E) Adopt secure development practices for in-house developed applications used by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications used by the licensee;

(F) Modify the information system in accordance with the licensee's information security program;

(G) Use effective controls, which may include multi-factor authentication procedures for any individual accessing nonpublic information;

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

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

(J) 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; and

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

(3) Include cybersecurity risks in the licensee's enterprise risk management process;

(4) Stay informed regarding emerging threats or vulnerabilities and use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

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

§431: -204 Oversight by board of directors. If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

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

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

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

(B) 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 information security program; and

(3) If executive management delegates any of its responsibilities under this part, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors specified in paragraph (2).

§431: -205 Oversight of third-party service provider arrangements. A licensee shall:

(1) Exercise due diligence in selecting its third-party service provider; and

(2) Where appropriate, 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; provided that encrypted nonpublic information is not accessible to or held by the third-party service provider within the meaning of this

paragraph if the third-party service provider does not possess the associated protective process or key necessary to assign meaning to the nonpublic information.

§431: -206 Program adjustments. 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.

§431: -207 Incident response plan. (a) As part of its information security 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) The 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.

§431: -208 Annual certification to commissioner. (a) Each insurer domiciled in the State shall annually submit to the commissioner a written statement by March 31, certifying that

the insurer is in compliance with the requirements set forth in this part.

(b) Each insurer shall maintain all records, schedules, and data supporting this certificate for a period of five years for examination by the commissioner.

(c) 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 those areas, systems, or processes. The documentation shall be available for inspection by the commissioner.

PART III. CYBERSECURITY EVENTS

§431: -301 Investigation of a cybersecurity event. (a) If the licensee learns that a cybersecurity event has or may have occurred, the licensee, outside vendor, or service provider designated to act on behalf of the licensee shall conduct a prompt investigation.

(b) During the investigation, the licensee, outside vendor, or service provider designated to act on behalf of the licensee shall, at a minimum, determine as much of the following information as possible:

(1) Whether a cybersecurity event has occurred;

(2) The nature and scope of the cybersecurity event; and

(3) Any nonpublic information that may have been involved in the cybersecurity event.

The licensee, outside vendor, or service provider designated to act on behalf of the licensee shall perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

(c) If the licensee provides nonpublic information to a third-party service provider and learns that a cybersecurity event has or may have impacted the licensee's nonpublic information in a system maintained by a third-party service provider, the licensee shall meet the requirements of subsection (b) or confirm and document that the third-party service provider has met the requirements of subsection (b).

(d) The licensee shall maintain records concerning all cybersecurity events for a period of at least five years from

the date of the cybersecurity event and shall produce those records upon demand of the commissioner.

§431: -302 Notification of a cybersecurity event. (a) Each licensee shall notify the commissioner as promptly as possible, but in no event later than three business days from a determination that a cybersecurity event impacting two hundred fifty or more consumers has occurred. If law enforcement officials instruct a licensee not to distribute information regarding a cybersecurity event, the licensee shall not be required to provide notification until instructed to do so by law enforcement officials. Notification shall be provided when either of the following criteria has been met:

(1) The licensee is domiciled in the State, in the case of an insurer, or the licensee's home state is Hawaii, in the case of an independent insurance producer; or

(2) The licensee reasonably believes that the nonpublic information involved is of two hundred fifty or more consumers residing in the State and is a cybersecurity event that has a reasonable likelihood of materially harming:

(A) Any consumer residing in the State; or

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

(b) The licensee shall provide as much of the following information as possible and practicable and as promptly as possible:

(1) The date of the cybersecurity event;

(2) The description of how the nonpublic information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any;

(3) How the cybersecurity event was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and, if so, how it was recovered;

(5) The identity of the source of the cybersecurity event;

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

(7) A description of the specific types of information acquired without authorization. For purposes of this paragraph, "specific types of information" means

particular data elements, including but not limited to types of medical information, types of financial information, or types of information allowing identification of the consumer;

(8) The period during which the information system was compromised by the cybersecurity event;

(9) The number of total consumers in the 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;

(10) 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;

(11) A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;

(12) 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; and

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

(c) The licensee shall provide the information in electronic form as directed by the commissioner.

(d) 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 concerning the cybersecurity event.

(e) This section shall not supersede any reporting requirements in chapter 487N.

§431: -303 Notification to consumers. The licensee shall comply with chapter 487N, as applicable, and provide a copy of the notice sent to consumers under chapter 487N to the commissioner when a licensee is required to notify the commissioner under section 431: -302.

§431: -304 Notice regarding cybersecurity events of third-party service providers. (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 the event as it would under section 431: -302.

(b) The computation of the 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 article 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 section 431: -301 or notice requirements imposed under this part.

§431: -305 Notice regarding cybersecurity events of reinsures to insurers. (a) 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 three business days of making the determination that a cybersecurity event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under chapter 487N and any other notification requirements relating to a cybersecurity event imposed under this part.

(c) In the case of a cybersecurity event impacting a licensee's nonpublic information in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat the event as it would under section 431: -302, unless the third-party service provider provides the notice required under section 431: -302 to the commissioner.

§431: -306 Notice regarding cybersecurity events of insurers to producers of record. (a) 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.

(b) The insurer is exempt from this obligation in instances where it does not have the current producer of record information for any individual consumer."

SECTION 3. Section 431:19-115, Hawaii Revised Statutes, is amended by amending subsection (a) to read as follows:

"(a) No insurance laws of this State other than those contained in this article, article 15, or specifically referenced in this article shall apply to captive insurance companies; provided that:

(1) Sections 431:3-302 to 431:3-304.5, 431:3-307, 431:3-401 to 431:3-409, 431:3-411, 431:3-412, and 431:3-414; articles 1, 2, 4A, 5, 6, 9A, 9B, 9C, 11, [~~and~~] 11A[~~.~~], and ; and chapter 431K shall apply to risk retention captive insurance companies; and

(2) Articles 1, 2, and 6 shall apply to class 5 companies."

SECTION 4. If any provision of this Act, or the application thereof to any person or circumstance, is held invalid, the invalidity does not affect other provisions or

applications of the Act that can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

SECTION 5. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 6. This Act shall take effect on July 1, 2050; provided that:

(1) Licensees, other than risk retention groups chartered and licensed in this State, shall have:

(A) One year from the effective date of this Act to implement sections 431: -201, 431: -202, 431: -203, 431: -204, 431: -206, 431: -207, and 431: -208, Hawaii Revised Statutes, established by section 1 of this Act; and

(B) Two years from the effective date of this Act to implement section 431: -205, Hawaii Revised Statutes, established by section 1 of this Act; and

(2) Risk retention groups chartered and licensed in this State shall have:

(A) Two years from the effective date of this Act to implement sections 431: -201, 431: -202, 431: -203, 431: -204, 431: -206, 431: -207, and 431: -208, Hawaii Revised Statutes, established by section 1 of this Act; and

(B) Three years from the effective date of this Act to implement section 431: -205, Hawaii Revised Statutes, established by section 1 of this Act.

S.B. NO. 1100 S.D. 1 H.D. 1

Report Title:
Insurance Data Security Model Law; National Association of Insurance Commissioners; Data Security; Information Security Program; Nonpublic Information; Cybersecurity Event

Description:
Adopts the National Association of Insurance Commissioners' Insurance Data Security Model Law to establish insurance data security standards for Hawaii insurance licensees. Effective 7/1/2050. (HD1)

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.