THE SENATE
THIRTY-FIRST LEGISLATURE, 2021
STATE OF HAWAII

S.B. NO. 1100
S.D. 1
H.D. 2

A BILL FOR AN ACT

RELATING TO INSURANCE DATA SECURITY.

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

1   SECTION 1. The legislature finds that the National

2 Association of Insurance Commissioners adopted the Insurance

3 Data Security Model Law in 2017 to strengthen existing data

4 privacy and consumer breach notification obligations of

5 insurance licensees. The National Association of Insurance

6 Commissioners strongly encourages that states enact this model

7 law by 2022, to avoid risking federal preemption of state laws

8 in this area. While some licensees may already have

9 cybersecurity policies and protocols in place, this Act will

10 ensure and formalize insurance data security protections for all

11 insurance licensees.

12   The purpose of this Act is to enact the National

13 Association of Insurance Commissioners Insurance Data Security

14 Model Law to establish the exclusive state standards applicable

15 to Hawaii insurance licensees for insurance data security, the

16 investigation of a cybersecurity event, and notification to the

17 commissioner.

1   SECTION 2. Chapter 431, Hawaii Revised Statutes, is

2 amended by adding a new article to be appropriately designated

3 and to read as follows:

4   **"ARTICLE**

5   **INSURANCE DATA SECURITY LAW**

6   **PART I. GENERAL PROVISIONS**

7   **§431: -101 Definitions**. As used in this article:

8   "Authorized individual" means an individual known to and

9 screened by the licensee and determined to be necessary and

10 appropriate to have access to the nonpublic information held by

11 the licensee and its information systems.

12   "Consumer" means an individual, including but not limited

13 to applicants, policyholders, insureds, beneficiaries,

14 claimants, and certificate holders, who is a resident of this

15 State and whose nonpublic information is in a licensee's

16 possession, custody, or control.

17   "Cybersecurity event" means an event resulting in

18 unauthorized access to, or disruption or misuse of, an

19 information system or nonpublic information stored on that

20 information system. "Cybersecurity event" does not include:

1   (1)   The unauthorized acquisition of encrypted nonpublic

2   information if the encryption, process, or key is not

3   also acquired, released, or used without

4   authorization; and

5   (2)   An event in which the licensee has determined that the

6   nonpublic information accessed by an unauthorized

7   person has not been used or released and has been

8   returned or destroyed.

9   "Encrypted" means the transformation of data into a form

10 that results in a low probability of assigning meaning without

11 the use of a protective process or key.

12   "Information security program" means the administrative,

13 technical, and physical safeguards that a licensee uses to

14 access, collect, distribute, process, protect, store, use,

15 transmit, dispose of, or otherwise handle nonpublic information.

16   "Information system" means a discrete set of electronic

17 information resources organized for the collection, processing,

18 maintenance, use, sharing, dissemination, or disposition of

19 electronic nonpublic information, as well as any specialized

20 systems, such as industrial controls systems, process controls

1 systems, telephone switching and private branch exchange

2 systems, and environmental control systems.

3 "Licensee" means every licensed insurer, producer, and any

4 other person licensed or required to be licensed, authorized or

5 required to be authorized, or registered or required to be

6 registered, under chapter 431 or 432, or holding a certificate

7 of authority under chapter 432D. "Licensee" does not include a

8 purchasing group or risk retention group chartered and licensed

9 in a state other than this State, or a licensee that is acting

10 as an assuming insurer that is domiciled in another state or

11 jurisdiction.

12 "Multi-factor authentication" means authentication through

13 verification of at least two of the following types of

14 authentication factors:

15   (1)   Knowledge factors, such as a password;

16   (2)   Possession factors, such as a token or text message on

17   a mobile phone; or

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

19 "Nonpublic information" means electronic information that

20 is not publicly available information and is:

1   (1) Any information concerning a consumer that, because of

2   name, number, personal mark, or other identifier, can

3   be used to identify the consumer, in combination with

4   any one or more of the following data elements:

5   (A) Social security number;

6   (B) Driver's license number or non-driver

7   identification card number;

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

9   number;

10   (D) Any security code, access code, or password that

11   would permit access to a consumer's financial

12   account; or

13   (E) Biometric records; or

14   (2) Any information or data subject to the Health

15   Insurance Portability and Accountability Act of 1996,

16   P.L. 104-191, except age or gender, in any form or

17   medium created by or derived from a health care

18   provider or a consumer that identifies a particular

19   consumer and that relates to:

1   (A)   The past, present, or future physical, mental, or

2   behavioral health or condition of any consumer or

3   a member of the consumer's family;

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

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

6   consumer.

7   "Person" means any individual or any non-governmental

8 entity, including but not limited to any non-governmental

9 partnership, corporation, branch, agency, or association.

10   "Publicly available information" means any information that

11 a licensee has a reasonable basis to believe is lawfully made

12 available to the general public from federal, state, or local

13 government records; widely distributed media; or disclosures to

14 the general public that are required to be made by federal,

15 state, or local law. For purposes of this definition, a

16 licensee has a reasonable basis to believe that information is

17 lawfully made available to the general public if the licensee

18 has taken steps to determine:

19   (1)   That the information is of the type that is available

20   to the general public; and

1   (2)   Whether a consumer can direct that the information not

2   be made available to the general public and, if so,

3   that the consumer has not done so.

4   "Risk assessment" means the risk assessment that each

5   licensee is required to conduct under section 431:   -202.

6   "State" means the State of Hawaii.

7   "Third-party service provider" means a person, not

8   otherwise defined as a licensee, that contracts with a licensee

9   to maintain, process, store, or otherwise is permitted access to

10   nonpublic information through its provision of services to the

11   licensee.

12   §431:   -102 **Powers of the commissioner.** (a)   The

13   licensee's domiciliary regulator shall have the power to examine

14   and investigate the affairs of any licensee to determine whether

15   the licensee has been or is engaged in any conduct in violation

16   of this article.

17   (b)   Any examination or investigation of a licensee

18   domiciled in the State shall be conducted pursuant to

19   section 431:2-301.7.

20   (c)   Whenever the commissioner has reason to believe that a

21   licensee has been or is engaged in conduct in the State that

1 violates this article, the commissioner may take action that is

2 necessary or appropriate to enforce the provisions of this

3 article.

4   **§431: -103 Confidentiality.** (a) Any documents,

5 materials, or other information in the control or possession of

6 the commissioner that is furnished by a licensee, or an employee

7 or agent thereof acting on behalf of the licensee pursuant to

8 sections 431: -208 and 431: -302, or that are obtained by

9 the commissioner in an examination or investigation pursuant to

10 section 431: -102, shall be confidential by law and

11 privileged, shall not be subject to chapter 92F, shall not be

12 subject to subpoena, and shall not be subject to discovery or

13 admissible as evidence in any private civil action; provided

14 that the commissioner may use the documents, materials, or other

15 information obtained in an examination or investigation in the

16 furtherance of any regulatory or legal action brought as a part

17 of the commissioner's duties.

18   (b) Neither the commissioner nor any person acting under

19 the direction of the commissioner shall be allowed or required

20 to testify in any private civil action concerning any

1 confidential documents, materials, or information subject to

2 subsection (a).

3   (c) To assist in the performance of the commissioner's

4 duties under this article, the commissioner may:

5   (1) Share documents, materials, or other information,

6   including the confidential and privileged documents,

7   materials, or information subject to subsection (a),

8   with other state, federal, and international

9   regulatory agencies; National Association of Insurance

10   Commissioners, its affiliates or subsidiaries; and

11   state, federal, and international law enforcement

12   authorities; provided that the recipient agrees in

13   writing to maintain the confidentiality and privileged

14   status of the document, material, or other

15   information;

16   (2) Receive documents, materials, or information,

17   including otherwise confidential and privileged

18   documents, materials, or information, from the

19   National Association of Insurance Commissioners, its

20   affiliates or subsidiaries, and from regulatory and

21   law enforcement officials of other foreign or domestic

1   jurisdictions; provided that the commissioner shall

2   maintain as confidential or privileged any document,

3   material, or information received with notice or the

4   understanding that it is confidential or privileged

5   under the laws of the jurisdiction that is the source

6   of the document, material, or information;

7   (3) Share documents, materials, or other information

8   subject to subsection (a) with a third-party

9   consultant or vendor; provided that the consultant or

10   vendor agrees in writing to maintain the

11   confidentiality and privileged status of the document,

12   material, or other information; and

13   (4) Enter into agreements governing sharing and use of

14   information consistent with this subsection.

15   (d) No waiver of any applicable privilege or claim of

16 confidentiality in the documents, materials, or information

17 shall occur as a result of disclosure to the commissioner under

18 this section or as a result of sharing as authorized in

19 subsection (c).

20   (e) Nothing in this article shall prohibit the

21 commissioner from releasing final, adjudicated actions that are

1   open to public inspection pursuant to chapter 92F to a database

2   or other clearinghouse service maintained by the National

3   Association of Insurance Commissioners, its affiliates, or

4   subsidiaries.

5   **§431:   -104 Exceptions.**   (a)   The following exceptions

6   shall apply to this article:

7   (1) A licensee with fewer than ten employees, including

8   any independent contractors, shall be exempt from

9   part II;

10   (2) A licensee subject to the Health Insurance Portability

11   and Accountability Act of 1996, Public Law 104-191,

12   that has established and maintains an information

13   security program pursuant to the statutes, rules,

14   regulations, procedures, or guidelines established

15   thereunder shall be considered to have met the

16   requirements of part II of this article; provided that

17   the licensee is compliant with and submits a written

18   statement certifying its compliance with the Health

19   Insurance Portability and Accountability Act of 1996,

20   Public Law 104-191; and

1   (3)   An employee, agent, representative, or designee of a

2   licensee, who is also a licensee, shall be exempt from

3   part II of this article and shall not be required to

4   develop its own information security program; provided

5   that the employee, agent, representative, or designee

6   is covered by the information security program of the

7   other licensee.

8   (b)   In the event that a licensee ceases to qualify for an

9   exception pursuant to this section, the licensee shall have one

10   hundred eighty days to comply with this article.

11   **§431: -105 Penalties.** In the case of a violation of

12   this article, a licensee may be penalized in accordance with

13   section 431:2-203.

14   **§431: -106 Private cause of action.** This article shall

15   not be construed to create or imply a private cause of action

16   for any violation of its provisions, and it shall not be

17   construed to curtail a private cause of action that would

18   otherwise exist in the absence of this article.

19   **§431: -107 Rules.** The commissioner may adopt rules

20   pursuant to chapter 91 as necessary to carry out the provisions

21   of this article.

1   PART II.   INFORMATION SECURITY PROGRAM

2   §431:   -201 **Implementation of an information security**

3   **program.** Commensurate with the size and complexity of the

4   licensee, the nature and scope of the licensee's activities,

5   including its use of third-party service providers, and the

6   sensitivity of the nonpublic information used by the licensee or

7   in the licensee's possession, custody, or control, each licensee

8   shall develop, implement, and maintain a comprehensive written

9   information security program based on the licensee's risk

10   assessment and that contains administrative, technical, and

11   physical safeguards for the protection of nonpublic information

12   and the licensee's information system.

13   §431:   -202 **Objectives of the information security**

14   **program; risk assessment.** (a) A licensee's information

15   security program shall be designed to:

16   (1) Protect the security and confidentiality of nonpublic

17   information and the security of the information

18   system;

19   (2) Protect against any threats or hazards to the security

20   or integrity of nonpublic information and the

21   information system;

1   (3) Protect against unauthorized access to or use of

2   nonpublic information, and minimize the likelihood of

3   harm to any consumer; and

4   (4) Define and periodically reevaluate a schedule for

5   retention of nonpublic information and a mechanism for

6   its destruction when no longer needed.

7   (b) Regarding risk assessment, the licensee shall:

8   (1) Designate one or more employees, an affiliate, or a

9   third-party service provider to act on behalf of the

10   licensee who is responsible for the information

11   security program;

12   (2) Identify reasonably foreseeable internal or external

13   threats that could result in unauthorized access,

14   transmission, disclosure, misuse, alteration, or

15   destruction of nonpublic information, including the

16   security of information systems and nonpublic

17   information that are accessible to or held by

18   third-party service providers;

19   (3) Assess the likelihood and potential damage of the

20   reasonably foreseeable internal or external threats,

1   taking into consideration the sensitivity of the

2   nonpublic information;

3 (4) Assess the sufficiency of policies, procedures,

4   information systems, and other safeguards in place to

5   manage the reasonably foreseeable internal or external

6   threats, including consideration of threats in each

7   relevant area of the licensee's operations, including:

8   (A) Employee training and management;

9   (B) Information systems, including network and

10   software design, as well as information

11   classification, governance, processing, storage,

12   transmission, and disposal; and

13   (C) Detecting, preventing, and responding to attacks,

14   intrusions, or other systems failures; and

15 (5) Implement information safeguards to manage the threats

16   identified in its ongoing assessment, and no less than

17   annually, assess the effectiveness of the safeguards'

18   key controls, systems, and procedures.

19 §431: -203 **Risk management.** Based on its risk

20 assessment, the licensee shall:

1   (1)   Design its information security program to mitigate

2   the identified risks, commensurate with the size and

3   complexity of the licensee's activities, including its

4   use of third-party service providers, and the

5   sensitivity of the nonpublic information used by the

6   licensee or in the licensee's possession, custody, or

7   control;

8   (2)   Determine which security measures listed in this

9   paragraph are appropriate and implement those security

10   measures:

11   (A)   Place access controls on information systems,

12   including controls to authenticate and permit

13   access only to authorized individuals to protect

14   against the unauthorized acquisition of nonpublic

15   information;

16   (B)   Identify and manage the data, personnel, devices,

17   systems, and facilities that enable the licensee

18   to achieve business purposes in accordance with

19   their relative importance to business objectives

20   and the licensee's risk strategy;

1   (C) Restrict access at physical locations containing

2   nonpublic information only to authorized

3   individuals;

4   (D) Protect by encryption or other appropriate means,

5   all nonpublic information while being transmitted

6   over an external network and all nonpublic

7   information stored on a laptop computer or other

8   portable computing or storage device or media;

9   (E) Adopt secure development practices for in-house

10   developed applications used by the licensee and

11   procedures for evaluating, assessing, or testing

12   the security of externally developed applications

13   used by the licensee;

14   (F) Modify the information system in accordance with

15   the licensee's information security program;

16   (G) Use effective controls, which may include

17   multi-factor authentication procedures for any

18   individual accessing nonpublic information;

19   (H) Regularly test and monitor systems and procedures

20   to detect actual and attempted attacks on, or

21   intrusions into, information systems;

S.B. NO. ₁₁₀₀
S.D. 1
H.D. 2

1   (I)   Include audit trails within the information

2   security program designed to detect and respond

3   to cybersecurity events and reconstruct material

4   financial transactions sufficient to support

5   normal operations and obligations of the

6   licensee;

7   (J)   Implement measures to protect against

8   destruction, loss, or damage of nonpublic

9   information due to environmental hazards, such as

10   fire and water damage or other catastrophes or

11   technological failures; and

12   (K)   Develop, implement, and maintain procedures for

13   the secure disposal of nonpublic information in

14   any format;

15   (3)   Include cybersecurity risks in the licensee's

16   enterprise risk management process;

17   (4)   Stay informed regarding emerging threats or

18   vulnerabilities and use reasonable security measures

19   when sharing information relative to the character of

20   the sharing and the type of information shared; and

1   (5) Provide its personnel with cybersecurity awareness

2   training that is updated as necessary to reflect risks

3   identified by the licensee in the risk assessment.

4   §431: -204 **Oversight by board of directors.** If the

5 licensee has a board of directors, the board or an appropriate

6 committee of the board shall, at a minimum:

7   (1) Require the licensee's executive management or its

8   delegates to develop, implement, and maintain the

9   licensee's information security program;

10   (2) Require the licensee's executive management or its

11   delegates to report in writing at least annually, the

12   following information:

13   (A) The overall status of the information security

14   program and the licensee's compliance with this

15   article; and

16   (B) Material matters related to the information

17   security program, addressing issues such as risk

18   assessment, risk management and control

19   decisions, third-party service provider

20   arrangements, results of testing, cybersecurity

21   events or violations and management's responses

1   thereto, and recommendations for changes in the

2   information security program; and

3   (3) If executive management delegates any of its

4   responsibilities under this part, it shall oversee the

5   development, implementation, and maintenance of the

6   licensee's information security program prepared by

7   the delegate and shall receive a report from the

8   delegate complying with the requirements of the report

9   to the board of directors specified in paragraph (2).

10   §431:   -205 **Oversight of third-party service provider**

11 **arrangements.** A licensee shall:

12   (1) Exercise due diligence in selecting its third-party

13   service provider; and

14   (2) Where appropriate, require a third-party service

15   provider to implement appropriate administrative,

16   technical, and physical measures to protect and secure

17   the information systems and nonpublic information that

18   are accessible to or held by the third-party service

19   provider; provided that encrypted nonpublic

20   information is not accessible to or held by the

21   third-party service provider within the meaning of

1   this paragraph if the third-party service provider

2   does not possess the associated protective process or

3   key necessary to assign meaning to the nonpublic

4   information.

5   §431: -206 **Program adjustments**. The licensee shall

6   monitor, evaluate, and adjust, as appropriate, the information

7   security program consistent with any relevant changes in

8   technology, the sensitivity of its nonpublic information,

9   internal or external threats to information, and the licensee's

10 own changing business arrangements, such as mergers and

11 acquisitions, alliances and joint ventures, outsourcing

12 arrangements, and changes to information systems.

13   §431: -207 **Incident response plan**. (a) As part of its

14 information security program, each licensee shall establish a

15 written incident response plan designed to promptly respond to

16 and recover from any cybersecurity event that compromises the

17 confidentiality, integrity, or availability of nonpublic

18 information in its possession, the licensee's information

19 systems, or the continuing functionality of any aspect of the

20 licensee's business or operations.

1   (b) The incident response plan shall address the following

2 areas:

3   (1) The internal process for responding to a cybersecurity

4   event;

5   (2) The goals of the incident response plan;

6   (3) The definition of clear roles, responsibilities, and

7   levels of decision-making authority;

8   (4) External and internal communications and information

9   sharing;

10   (5) Identification of requirements for the remediation of

11   any identified weaknesses in information systems and

12   associated controls;

13   (6) Documentation and reporting regarding cybersecurity

14   events and related incident response activities; and

15   (7) The evaluation and revision, as necessary, of the

16   incident response plan following a cybersecurity

17   event.

18   §431:   -208 **Annual certification to commissioner.** (a)

19 Each licensee domiciled in the State shall annually submit to

20 the commissioner a written statement by March 31, certifying

1 that the licensee is in compliance with the requirements set

2 forth in this part.

3   (b) Each licensee shall maintain all records, schedules,

4 and data supporting this certificate for a period of five years

5 for examination by the commissioner.

6   (c) To the extent a licensee has identified areas,

7 systems, or processes that require material improvement,

8 updating, or redesign, the licensee shall document the

9 identification and the remedial efforts planned and underway to

10 address those areas, systems, or processes. The documentation

11 shall be available for inspection by the commissioner.

12   **PART III. CYBERSECURITY EVENTS**

13   **§431: -301 Investigation of a cybersecurity event.** (a)

14 If the licensee learns that a cybersecurity event has or may

15 have occurred, the licensee or third-party service provider

16 designated to act on behalf of the licensee shall conduct a

17 prompt investigation.

18   (b) During the investigation, the licensee or third-party

19 service provider designated to act on behalf of the licensee

20 shall, at a minimum, determine as much of the following

21 information as possible:

1   (1)   Whether a cybersecurity event has occurred;

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

3   (3)   Any nonpublic information that may have been involved

4   in the cybersecurity event.

5   The licensee or third-party service provider designated to

6 act on behalf of the licensee shall perform or oversee

7 reasonable measures to restore the security of the information

8 systems compromised in the cybersecurity event to prevent

9 further unauthorized acquisition, release, or use of nonpublic

10 information in the licensee's possession, custody, or control.

11   (c)   If the licensee provides nonpublic information to a

12 third-party service provider and learns that a cybersecurity

13 event has or may have impacted the licensee's nonpublic

14 information in a system maintained by a third-party service

15 provider, the licensee shall meet the requirements of

16 subsection (b) or confirm and document that the third-party

17 service provider has met the requirements of subsection (b).

18   (d)   The licensee shall maintain records concerning all

19 cybersecurity events for a period of at least five years from

20 the date of the cybersecurity event and shall produce those

21 records upon demand of the commissioner.

1   §431:   -302 **Notification of a cybersecurity event.** (a)

2 Each licensee shall notify the commissioner as promptly as

3 possible, but in no event later than three business days from a

4 determination that a cybersecurity event impacting two hundred

5 fifty or more consumers has occurred. If law enforcement

6 officials instruct a licensee not to distribute information

7 regarding a cybersecurity event, the licensee shall not be

8 required to provide notification until instructed to do so by

9 law enforcement officials. Notification shall be provided when

10 either of the following criteria has been met:

11   (1)   The licensee is domiciled in the State, in the case of

12   an insurer, or the licensee's home state is Hawaii, in

13   the case of an independent insurance producer; or

14   (2)   The licensee reasonably believes that the nonpublic

15   information involved is of two hundred fifty or more

16   consumers residing in the State and is a cybersecurity

17   event that has a reasonable likelihood of materially

18   harming:

19   (A)   Any consumer residing in the State; or

20   (B)   Any material part of the normal operation of the

21   licensee.

1   (b)   The licensee shall provide as much of the following

2   information as possible and practicable and as promptly as

3   possible:

4   (1)   The date of the cybersecurity event;

5   (2)   The description of how the nonpublic information was

6   exposed, lost, stolen, or breached, including the

7   specific roles and responsibilities of third-party

8   service providers, if any;

9   (3)   How the cybersecurity event was discovered;

10   (4)   Whether any lost, stolen, or breached information has

11   been recovered and, if so, how it was recovered;

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

13   (6)   Whether the licensee has filed a police report or has

14   notified any regulatory, government, or law

15   enforcement agencies and, if so, when the notification

16   was provided;

17   (7)   A description of the specific types of information

18   acquired without authorization. For purposes of this

19   paragraph, "specific types of information" means

20   particular data elements, including but not limited to

21   types of medical information, types of financial

1   information, or types of information allowing

2   identification of the consumer;

3   (8)   The period during which the information system was

4   compromised by the cybersecurity event;

5   (9)   The number of total consumers in the State affected by

6   the cybersecurity event. The licensee shall provide

7   the best estimate in the initial notification to the

8   commissioner and update this estimate with each

9   subsequent notification to the commissioner pursuant

10   to this section;

11   (10)   The results of any internal review identifying a lapse

12   in either automated controls or internal procedures,

13   or confirming that all automated controls or internal

14   procedures were followed;

15   (11)   A description of efforts being undertaken to remediate

16   the situation that permitted the cybersecurity event

17   to occur;

18   (12)   A copy of the licensee's privacy policy and a

19   statement outlining the steps the licensee will take

20   to investigate and notify consumers affected by the

21   cybersecurity event; and

1   (13) The name of a contact person who is both familiar with

2   the cybersecurity event and authorized to act for the

3   licensee.

4   (c) The licensee shall provide the information in

5 electronic form as directed by the commissioner.

6   (d) The licensee shall have a continuing obligation to

7 update and supplement initial and subsequent notifications to

8 the commissioner regarding material changes to previously

9 provided information concerning the cybersecurity event.

10   (e) This section shall not supersede any reporting

11 requirements in chapter 487N.

12   **§431: -303 Notification to consumers.** The licensee

13 shall comply with chapter 487N, as applicable, and provide a

14 copy of the notice sent to consumers under chapter 487N to the

15 commissioner when a licensee is required to notify the

16 commissioner under section 431: -302.

17   **§431: -304 Notice regarding cybersecurity events of**

18 **third-party service providers.** (a) In the case of a

19 cybersecurity event impacting a licensee's nonpublic information

20 in a system maintained by a third-party service provider, of

21 which the licensee has become aware, the licensee shall treat

1   the event as it would under section 431:   -302 unless the

2   third-party service provider provides the notice required under

3   section 431:   -302.

4   (b) The computation of the licensee's deadlines shall

5   begin on the day after the third-party service provider notifies

6   the licensee of the cybersecurity event or the licensee

7   otherwise has actual knowledge of the cybersecurity event,

8   whichever is sooner.

9   (c) Nothing in this article shall prevent or abrogate an

10 agreement between a licensee and another licensee, a third-party

11 service provider, or any other party to fulfill any of the

12 investigation requirements imposed under section 431:   -301 or

13 notice requirements imposed under this part.

14   §431:   -305 **Notice regarding cybersecurity events of**

15 **reinsures to insurers.** (a) In the case of a cybersecurity

16 event involving nonpublic information that is used by the

17 licensee that is acting as an assuming insurer or in the

18 possession, custody, or control of a licensee that is acting as

19 an assuming insurer and that does not have a direct contractual

20 relationship with the affected consumers, the assuming insurer

21 shall notify its affected ceding insurers and the commissioner

1 of its state of domicile within three business days of making

2 the determination that a cybersecurity event has occurred.

3   (b) In the case of a cybersecurity event involving

4 nonpublic information that is in the possession, custody, or

5 control of a third-party service provider of a licensee that is

6 an assuming insurer, the assuming insurer shall notify its

7 affected ceding insurers and the commissioner of its state of

8 domicile within three business days of receiving notice from its

9 third-party service provider that a cybersecurity event has

10 occurred.

11   (c) The ceding insurers that have a direct contractual

12 relationship with affected consumers shall fulfill the consumer

13 notification requirements imposed under chapter 487N and any

14 other notification requirements relating to a cybersecurity

15 event imposed under this part.

16   §431:   -306 **Notice regarding cybersecurity events of**

17 **insurers to producers of record.** (a) In the case of a

18 cybersecurity event involving nonpublic information that is in

19 the possession, custody, or control of a licensee that is an

20 insurer or its third-party service provider, and for which a

21 consumer accessed the insurer's services through an independent

1 insurance producer, the insurer shall notify the producers of

2 record of all affected consumers as soon as practicable as

3 directed by the commissioner.

4   (b) The insurer is exempt from this obligation in

5 instances where it does not have the current producer of record

6 information for any individual consumer."

7   SECTION 3. Section 431:19-115, Hawaii Revised Statutes, is

8 amended by amending subsection (a) to read as follows:

9   "(a) No insurance laws of this State other than those

10 contained in this article, article 15, or specifically

11 referenced in this article shall apply to captive insurance

12 companies; provided that:

13   (1) Sections 431:3-302 to 431:3-304.5, 431:3-307,

14   431:3-401 to 431:3-409, 431:3-411, 431:3-412, and

15   431:3-414; articles 1, 2, 4A, 5, 6, 9A, 9B, 9C, 11,

16   [and] 11A[ː], and ____; and chapter 431K shall apply to

17   risk retention captive insurance companies; and

18   (2) Articles 1, 2, and 6 shall apply to class 5

19   companies."

20   SECTION 4. If any provision of this Act, or the

21 application thereof to any person or circumstance, is held

1 invalid, the invalidity does not affect other provisions or

2 applications of the Act that can be given effect without the

3 invalid provision or application, and to this end the provisions

4 of this Act are severable.

5   SECTION 5. Statutory material to be repealed is bracketed

6 and stricken. New statutory material is underscored.

7   SECTION 6. This Act shall take effect on July 1, 2050;

8 provided that:

9   (1)   Licensees, other than risk retention groups chartered

10   and licensed in this State, shall have:

11   (A) One year from the effective date of this Act to

12   implement sections 431: -201, 431: -202,

13   431: -203, 431: -204, 431: -206,

14   431: -207, and 431: -208, Hawaii Revised

15   Statutes, established by section 2 of this Act;

16   and

17   (B) Two years from the effective date of this Act to

18   implement section 431: -205, Hawaii Revised

19   Statutes, established by section 2 of this Act;

20   and

1   (2)   Risk retention groups chartered and licensed in this

2   State shall have:

3   (A)   Two years from the effective date of this Act to

4   implement sections 431:   -201, 431:   -202,

5   431:   -203, 431:   -204, 431:   -206,

6   431:   -207, and 431:   -208, Hawaii Revised

7   Statutes, established by section 2 of this Act;

8   and

9   (B)   Three years from the effective date of this Act

10   to implement section 431:   -205, Hawaii Revised

11   Statutes, established by section 2 of this Act.

S.B. NO. 1100
S.D. 1
H.D. 2

Report Title:
Insurance Data Security Model Law; Data Security; Nonpublic Information; Cybersecurity Event

Description:
Enacts 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. (HD2)

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

2021-2786 SB1100 HD2 HMSO