

---

---

# A BILL FOR AN ACT

RELATING TO INSURANCE DATA SECURITY.

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

1 SECTION 1. 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 A**

5 **INSURANCE DATA SECURITY LAW**

6 **§431:A-A Definitions.** As used in this article:

7 "Authorized individual" means an individual known to and  
8 screened by the licensee and determined to be necessary and  
9 appropriate to have access to the nonpublic information held by  
10 the licensee and its information systems.

11 "Commissioner" means the insurance commissioner of this  
12 State.

13 "Consumer" means an individual, including, but not limited  
14 to, applicants, policyholders, insureds, beneficiaries,  
15 claimants, and certificate holders, who is a resident of this  
16 State and whose nonpublic information is in a licensee's  
17 possession, custody, or control.

H.B. NO. 946

1 "Cybersecurity event" means an event resulting in  
2 unauthorized access to, disruption or misuse of, an information  
3 system or information stored on that information system.

4 "Cybersecurity event" shall not include:

5 (1) Unauthorized acquisition of encrypted nonpublic  
6 information if the encryption, process, or key is not  
7 also acquired, released, or used without  
8 authorization; and

9 (2) An event in which the licensee has determined that the  
10 nonpublic information accessed by an unauthorized  
11 person has not been used or released and has been  
12 returned or destroyed.

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

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

20 "Information system" means a discrete set of electronic  
21 information resources organized for the collection, processing,  
22 maintenance, use, sharing, dissemination, or disposition of

H.B. NO. 946

1 electronic information, as well as any specialized system such  
2 as industrial controls systems, process controls systems,  
3 telephone switching and private branch exchange systems, and  
4 environmental control systems.

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

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

- 17 (1) Knowledge factors, such as a password;
- 18 (2) Possession factors, such as a token or text message on  
19 a mobile phone; or
- 20 (3) Inherence factors, such as a biometric characteristic.

21 "Nonpublic information" means information that is not  
22 publicly available information and is:

H.B. NO. 946

- 1           (1) Business-related information of a licensee, whose  
2           tampering, unauthorized disclosure, access, or use  
3           would cause a material adverse impact to the business,  
4           operations, or security of the licensee; or
- 5           (2) Any information concerning a consumer which, because  
6           of name, number, personal mark, or other identifier,  
7           can be used to identify the consumer, in combination  
8           with any one or more of the following data elements:
- 9           (A) Social security number;
- 10           (B) Driver's license number or non-driver  
11           identification card number;
- 12           (C) Account number, credit, or debit card number;
- 13           (D) Any security code, access code, or password that  
14           would permit access to a consumer's financial  
15           account; or
- 16           (E) Biometric records; or
- 17           (3) Any information or data, except age or gender, in any  
18           form or medium created by or derived from a health  
19           care provider or a consumer and that relates to:
- 20           (A) The past, present, or future physical, mental, or  
21           behavioral health or condition of any consumer or  
22           a member of the consumer's family;

H.B. NO. 946

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

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

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

7 "Publicly available information" means any information that  
8 a licensee has a reasonable basis to believe is lawfully made  
9 available to the general public from:

10 (1) Federal, state, or local government records;

11 (2) Widely distributed media; or

12 (3) Disclosures to the general public that are required to  
13 be made by federal, state, or local law.

14 For purposes of this definition, a licensee has a reasonable  
15 basis to believe that information is lawfully made available to  
16 the general public if the licensee has taken steps to determine:

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

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

H.B. NO. 946

1 "Risk assessment" means the risk assessment that each  
2 licensee is required to conduct under section 431:A-C.

3 "State" means the State of Hawaii.

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

9 **§431:A-B Implementation of information security program.**

10 Commensurate with the size and complexity of the licensee, the  
11 nature and scope of the licensee's activities, including its use  
12 of third-party service providers, and the sensitivity of the  
13 nonpublic information used by the licensee or in the licensee's  
14 possession, custody, or control, each licensee shall develop,  
15 implement, and maintain a comprehensive written information  
16 security program based on the licensee's risk assessment and  
17 that contains administrative, technical, and physical safeguards  
18 for the protection of nonpublic information and the licensee's  
19 information system.

20 **§431:A-C Objectives of information security program. (a)**

21 A licensee's information security program shall be designed to:

H.B. NO. 946

- 1 (1) Protect the security and confidentiality of nonpublic  
2 information and the security of the information  
3 system;
- 4 (2) Protect against any threats or hazards to the security  
5 or integrity of nonpublic information and the  
6 information system;
- 7 (3) Protect against unauthorized access to or use of  
8 nonpublic information, and minimize the likelihood of  
9 harm to any consumer; and
- 10 (4) Define and periodically reevaluate a schedule for  
11 retention of nonpublic information and a mechanism for  
12 its destruction when no longer needed.
- 13 (b) Regarding risk assessment, the licensee shall:
- 14 (1) Designate one or more employees, an affiliate, or an  
15 outside vendor designated to act on behalf of the  
16 licensee who is responsible for the information  
17 security program;
- 18 (2) Identify reasonably foreseeable internal or external  
19 threats that could result in unauthorized access,  
20 transmission, disclosure, misuse, alteration or  
21 destruction of nonpublic information, including the  
22 security of information systems and nonpublic

H.B. NO. 946

- 1 information that are accessible to or held by third-  
2 party service providers;
- 3 (3) Assess the likelihood and potential damage of these  
4 threats, taking into consideration the sensitivity of  
5 the nonpublic information;
- 6 (4) Assess the sufficiency of policies, procedures,  
7 information systems, and other safeguards in place to  
8 manage these threats, including consideration of  
9 threats in each relevant area of the licensee's  
10 operations, including:
- 11 (A) Employee training and management;
- 12 (B) Information systems, including network and  
13 software design, as well as information  
14 classification, governance, processing, storage,  
15 transmission, and disposal; and
- 16 (C) Detecting, preventing, and responding to attacks,  
17 intrusions, or other systems failures; and
- 18 (5) Implement information safeguards to manage the threats  
19 identified in its ongoing assessment, and no less than  
20 annually, assess the effectiveness of the safeguards'  
21 key controls, systems, and procedures.



H.B. NO. 946

1           **§431:A-D Risk management.** Based on its risk assessment,  
2 the licensee shall:

3           (1) Design its information security program to mitigate  
4 the identified risks, commensurate with the size and  
5 complexity of the licensee's activities, including its  
6 use of third-party service providers, and the  
7 sensitivity of the nonpublic information used by the  
8 licensee or in the licensee's possession, custody, or  
9 control;

10          (2) Determine which security measures listed below are  
11 appropriate and implement such security measures:

12           (A) Place access controls on information systems,  
13 including controls to authenticate and permit  
14 access only to authorized individuals to protect  
15 against the unauthorized acquisition of nonpublic  
16 information;

17           (B) Identify and manage the data, personnel, devices,  
18 systems, and facilities that enable the  
19 organization to achieve business purposes in  
20 accordance with their relative importance to  
21 business objectives and the organization's risk  
22 strategy;

H.B. NO. 946

- 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 multi-  
17 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;

H.B. NO. 946

- 1 (I) Include audit trails within the information  
2 security program designed to detect and respond  
3 to cybersecurity events and designed to  
4 reconstruct material financial transactions  
5 sufficient to support normal operations and  
6 obligations of the 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
- 21 (5) Provide its personnel with cybersecurity awareness

H.B. NO. 946

1 training that is updated as necessary to reflect risks  
2 identified by the licensee in the risk assessment.

3 **§431:A-E Oversight by board of directors.** If the licensee  
4 has a board of directors, the board or an appropriate committee  
5 of the board shall, at a minimum:

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

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

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

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

H.B. NO. 946

1           (3) If executive management delegates any of its  
2           responsibilities under sections 431:A-B through 431:A-  
3           I, it shall oversee the development, implementation,  
4           and maintenance of the licensee's information security  
5           program prepared by the delegate and shall receive a  
6           report from the delegate complying with the  
7           requirements of the report to the board of directors  
8           above.

9           **§431:A-F Oversight of third-party service provider**

10          **arrangements.** A licensee shall:

- 11           (1) Exercise due diligence in selecting its third-party  
12           service provider; and
- 13           (2) Require a third-party service provider to implement  
14           appropriate administrative, technical, and physical  
15           measures to protect and secure the information systems  
16           and nonpublic information that are accessible to or  
17           held by the third-party service provider.

18          **§431:A-G Program adjustments.** The licensee shall monitor,  
19          evaluate, and adjust, as appropriate, the information security  
20          program consistent with any relevant changes in technology, the  
21          sensitivity of its nonpublic information, internal or external  
22          threats to information, and the licensee's own changing business

H.B. NO. 946

1 arrangements, such as mergers and acquisitions, alliances and  
2 joint ventures, outsourcing arrangements, and changes to  
3 information systems.

4       **§431:A-H Incident response plan.** (a) As part of its  
5 information security program, each licensee shall establish a  
6 written incident response plan designed to promptly respond to  
7 and recover from any cybersecurity event that compromises the  
8 confidentiality, integrity, or availability of nonpublic  
9 information in its possession, the licensee's information  
10 systems, or the continuing functionality of any aspect of the  
11 licensee's business or operations.

12       (b) The incident response plan shall address the following  
13 areas:

- 14       (1) The internal process for responding to a cybersecurity  
15 event;
- 16       (2) The goals of the incident response plan;
- 17       (3) The definition of clear roles, responsibilities, and  
18 levels of decision-making authority;
- 19       (4) External and internal communications and information  
20 sharing;

H.B. NO. 946

- 1           (5) Identification of requirements for the remediation of  
2           any identified weaknesses in information systems and  
3           associated controls;
- 4           (6) Documentation and reporting regarding cybersecurity  
5           events and related incident response activities; and
- 6           (7) The evaluation and revision, as necessary, of the  
7           incident response plan following a cybersecurity  
8           event.

9           **§431:A-I Annual certification to commissioner.** (a) Each  
10 insurer domiciled in this State shall annually submit to the  
11 commissioner a written statement by February 15, certifying that  
12 the insurer is in compliance with the requirements set forth in  
13 sections 431:A-B through 431:A-I.

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

17           (c) To the extent an insurer has identified areas,  
18 systems, or processes that require material improvement,  
19 updating, or redesign, the insurer shall document the  
20 identification and the remedial efforts planned and underway to  
21 address those areas, systems, or processes. The documentation  
22 shall be available for inspection by the commissioner.

H.B. NO. 946

1           **§431:A-J Investigation of a cybersecurity event.** (a) If  
2 the licensee learns that a cybersecurity event has or may have  
3 occurred, the licensee, outside vendor, or service provider  
4 designated to act on behalf of the licensee shall conduct a  
5 prompt investigation.

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

- 10           (1) Determine whether a cybersecurity event has occurred;  
11           (2) Assess the nature and scope of the cybersecurity  
12           event;  
13           (3) Identify any nonpublic information that may have been  
14           involved in the cybersecurity event; and  
15           (4) Perform or oversee reasonable measures to restore the  
16           security of the information systems compromised in the  
17           cybersecurity event to prevent further unauthorized  
18           acquisition, release, or use of nonpublic information  
19           in the licensee's possession, custody, or control.

20           (c) If the licensee learns that a cybersecurity event has  
21 or may have occurred in a system maintained by a third-party  
22 service provider, the licensee will complete the steps listed in



H.B. NO. 946

1 subsection (b) or confirm and document that the third-party  
2 service provider has completed those steps.

3 (d) The licensee shall maintain records concerning all  
4 cybersecurity events for a period of at least five years from  
5 the date of the cybersecurity event and shall produce those  
6 records upon demand of the commissioner.

7 **§431:A-K Notification of a cybersecurity event.** (a) Each  
8 licensee shall notify the commissioner as promptly as possible,  
9 but in no event later than seventy-two hours from a  
10 determination that a cybersecurity event has occurred, when  
11 either of the following criteria has been met:

12 (1) This State is the licensee's state of domicile, in the  
13 case of an insurer, or this State is the licensee's  
14 home state, in the case of a producer; or

15 (2) The licensee reasonably believes that the nonpublic  
16 information involved is of 250 or more consumers  
17 residing in this State and that is either of the  
18 following:

19 (A) A cybersecurity event impacting the licensee, in  
20 which notice is required to be provided to any  
21 government body, self-regulatory agency, or any

H.B. NO. 946

1 other supervisory body pursuant to any state or  
2 federal law; or

3 (B) A cybersecurity event that has a reasonable  
4 likelihood of materially harming:

5 (i) Any consumer residing in this State; or

6 (ii) Any material part of the normal operation of  
7 the licensee.

8 (b) The licensee shall provide as much of the following  
9 information as possible:

10 (1) Date of the cybersecurity event;

11 (2) Description of how the information was exposed, lost,  
12 stolen, or breached, including the specific roles and  
13 responsibilities of third-party service providers, if  
14 any;

15 (3) How the cybersecurity event was discovered;

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

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

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

H.B. NO. 946

- 1           (7) Description of the specific types of information  
2           acquired without authorization. "Specific types of  
3           information" means particular data elements,  
4           including, but not limited to, types of medical  
5           information, types of financial information, or types  
6           of information allowing identification of the  
7           consumer;
- 8           (8) The period during which the information system was  
9           compromised by the cybersecurity event;
- 10          (9) The number of total consumers in this State affected  
11          by the cybersecurity event. The licensee shall  
12          provide the best estimate in the initial report to the  
13          commissioner and update this estimate with each  
14          subsequent report to the commissioner pursuant to this  
15          section;
- 16          (10) The results of any internal review identifying a lapse  
17          in either automated controls or internal procedures,  
18          or confirming that all automated controls or internal  
19          procedures were followed;
- 20          (11) Description of efforts being undertaken to remediate  
21          the situation that permitted the cybersecurity event  
22          to occur;

H.B. NO. 946

1           (12) A copy of the licensee's privacy policy and a  
2                   statement outlining the steps the licensee will take  
3                   to investigate and notify consumers affected by the  
4                   cybersecurity event; and

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

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

10          (d) The licensee shall have a continuing obligation to  
11               update and supplement initial and subsequent notifications to  
12               the commissioner concerning the cybersecurity event.

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

15           **§431:A-L Notification to consumers.** The licensee shall  
16               comply with chapter 487N, as applicable, and provide a copy of  
17               the notice sent to consumers under that chapter to the  
18               commissioner when a licensee is required to notify the  
19               commissioner under section 431:A-K.

20           **§431:A-M Notice regarding cybersecurity events of third-**  
21           **party service providers.** (a) In the case of a cybersecurity  
22               event in a system maintained by a third-party service provider,

H.B. NO. 946

1 of which the licensee has become aware, the licensee shall treat  
2 the event as it would under section 431:A-K.

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

8 (c) Nothing in this article shall prevent or abrogate an  
9 agreement between a licensee and another licensee, a third-party  
10 service provider, or any other party to fulfill any of the  
11 investigation requirements imposed under section 431:A-J or  
12 notice requirements imposed under sections 431:A-K through  
13 431:A-O.

14 **§431:A-N 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

H.B. NO. 946

1 of its state of domicile within seventy-two hours of making the  
2 determination that a cybersecurity event has occurred.

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

8 (c) In the case of a cybersecurity event involving  
9 nonpublic information that is in the possession, custody, or  
10 control of a third-party service provider of a licensee that is  
11 an assuming insurer, the assuming insurer shall notify its  
12 affected ceding insurers and the commissioner of its state of  
13 domicile within seventy-two hours of receiving notice from its  
14 third-party service provider that a cybersecurity event has  
15 occurred.

16 (d) The ceding insurers that have a direct contractual  
17 relationship with affected consumers shall fulfill the consumer  
18 notification requirements imposed under chapter 487N and any  
19 other notification requirements relating to a cybersecurity  
20 event imposed under this article.

21 **§431:A-0 Notice regarding cybersecurity events of insurers**  
22 **to producers of record.** (a) In the case of a cybersecurity

H.B. NO. 946

1 event involving nonpublic information that is in the possession,  
2 custody, or control of a licensee that is an insurer or its  
3 third-party service provider and for which a consumer accessed  
4 the insurer's services through an independent insurance  
5 producer, the insurer shall notify the producers of record of  
6 all affected consumers as soon as practicable as directed by the  
7 commissioner.

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

11 **§431:A-P Powers of the commissioner.** (a) The  
12 commissioner shall have power to examine and investigate the  
13 affairs of any licensee to determine whether the licensee has  
14 been or is engaged in any conduct in violation of this article.

15 (b) This power is in addition to the powers that the  
16 commissioner has under section 431:2-208. Any investigation or  
17 examination shall be conducted pursuant to section 431:2-301.7.

18 (c) Whenever the commissioner has reason to believe that a  
19 licensee has been or is engaged in conduct in this State that  
20 violates this article, the commissioner may take action that is  
21 necessary or appropriate to enforce the provisions of this  
22 article.

H.B. NO. 946

1           **§431:A-Q Confidentiality.** (a) Any documents, materials,  
2 or other information in the control or possession of the  
3 commissioner that is furnished by a licensee, or an employee or  
4 agent thereof acting on behalf of the licensee pursuant to  
5 sections 431:A-I and 431:A-K(b)(2), (3), (4), (5), (8), (10),  
6 and (11), or that are obtained by the commissioner in an  
7 investigation or examination pursuant to section 431:A-P shall  
8 be confidential by law and privileged, shall not be subject to  
9 chapter 92F, shall not be subject to subpoena, and shall not be  
10 subject to discovery or admissible in evidence in any private  
11 civil action. However, the commissioner is authorized to use  
12 the documents, materials, or other information in the  
13 furtherance of any regulatory or legal action brought as a part  
14 of the commissioner's duties.

15           (b) Neither the commissioner nor any person acting under  
16 the direction of the commissioner shall be permitted or required  
17 to testify in any private civil action concerning any  
18 confidential documents, materials, or information subject to  
19 subsection (a).

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



H.B. NO. 946

- 1           (1) May share documents, materials, or other information,  
2                   including the confidential and privileged documents,  
3                   materials, or information subject to subsection (a),  
4                   with other state, federal, and international  
5                   regulatory agencies, with the National Association of  
6                   Insurance Commissioners, its affiliates or  
7                   subsidiaries, and with state, federal, and  
8                   international law enforcement authorities; provided  
9                   that the recipient agrees in writing to maintain the  
10                  confidentiality and privileged status of the document,  
11                  material, or other information;
- 12           (2) May receive documents, materials, or information,  
13                   including otherwise confidential and privileged  
14                   documents, materials, or information, from the  
15                   National Association of Insurance Commissioners, its  
16                   affiliates or subsidiaries, and from regulatory and  
17                   law enforcement officials of other foreign or domestic  
18                   jurisdictions, and shall maintain as confidential or  
19                   privileged any document, material, or information  
20                   received with notice or the understanding that it is  
21                   confidential or privileged under the laws of the

H.B. NO. 946

1 jurisdiction that is the source of the document,  
2 material, or information;

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

9 (4) May enter into agreements governing sharing and use of  
10 information consistent with this subsection.

11 (d) No waiver of any applicable privilege or claim of  
12 confidentiality in the documents, materials, or information  
13 shall occur as a result of disclosure to the commissioner under  
14 this section or as a result of sharing as authorized in  
15 subsection (c).

16 (e) Nothing in this article shall prohibit the  
17 commissioner from releasing final adjudicated actions that are  
18 open to public inspection pursuant to chapter 92F to a database  
19 or other clearinghouse service maintained by the National  
20 Association of Insurance Commissioners, its affiliates, or  
21 subsidiaries.

H.B. NO. 946

1           **§431:A-R Exceptions.** (a) The following exceptions shall  
2 apply to this article:

3           (1) A licensee with fewer than ten employees, including  
4 any independent contractors, is exempt from sections  
5 431:A-B through 431:A-I;

6           (2) A licensee subject to the Health Insurance Portability  
7 and Accountability Act of 1996 that has established  
8 and maintains an information security program pursuant  
9 to the statutes, rules, regulations, procedures, or  
10 guidelines established thereunder will be considered  
11 to have met the requirements of sections 431:A-B  
12 through 431:A-I; provided that the licensee is  
13 compliant with and submits a written statement  
14 certifying its compliance with the same;

15           (3) An employee, agent, representative, or designee of a  
16 licensee, who is also a licensee, is exempt from  
17 sections 431:A-B through 431:A-I and need not develop  
18 its own information security program to the extent  
19 that the employee, agent, representative, or designee  
20 is covered by the information security program of the  
21 other licensee.

H.B. NO. 946

1 (b) In the event that a licensee ceases to qualify for an  
2 exception, the licensee shall have 180 days to comply with this  
3 article.

4 **§431:A-S Penalties.** In the case of a violation of this  
5 article, a licensee may be penalized in accordance with section  
6 431:2-203.

7 **§431:A-T Private cause of action.** This article may not be  
8 construed to create or imply a private cause of action for  
9 violation of its provisions, and it may not be construed to  
10 curtail a private cause of action that would otherwise exist in  
11 the absence of this article.

12 **§431:A-U Rules.** The commissioner may, in accordance with  
13 chapter 91, adopt rules as are necessary to carry out the  
14 provisions of this article."

15 SECTION 2. Section 431:19-115, Hawaii Revised Statutes, is  
16 amended by amending subsection (a) to read as follows:

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

21 (1) Sections 431:3-302 to 431:3-304.5, 431:3-307, 431:3-  
22 401 to 431:3-409, 431:3-411, 431:3-412, and 431:3-414;

H.B. NO. 946

1 articles 1, 2, 4A, 5, 6, 9A, 9B, 9C, 11, [~~and~~] 11A[~~+~~],  
2 and 431:A; and chapter 431K shall apply to risk  
3 retention captive insurance companies; and  
4 (2) Articles 1, 2, and 6 shall apply to class 5  
5 companies."

6 SECTION 3. If any provision of this Act, or the  
7 application thereof to any person or circumstance, is held  
8 invalid, the invalidity does not affect other provisions or  
9 applications of the Act that can be given effect without the  
10 invalid provision or application, and to this end the provisions  
11 of this Act are severable.

12 SECTION 4. In codifying the new article and sections added  
13 to chapter 431, Hawaii Revised Statutes, by section 1 of this  
14 Act, the revisor of statutes shall substitute appropriate  
15 article and section numbers for the letters used in designating  
16 and referring to the new article and sections in this Act.

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

19 SECTION 6. This Act shall take effect upon its approval;  
20 provided that licensees shall have one year from the effective  
21 date of this Act to implement sections 431:A-B through 431:A-I  
22 in section 1 of this Act, except that licensees shall have two

H.B. NO. 946

1 years from the effective date of this Act to implement section  
2 431:A-F in section 1 of this Act.

3

4

INTRODUCED BY: \_\_\_\_\_

*am*

5

BY REQUEST

JAN 25 2021

# H.B. NO. 946

**Report Title:**

Insurance Data Security Law; Data Security; Information Security Program; Nonpublic Information; Cybersecurity Event; Chapter 431

**Description:**

Adopts the National Conference of Insurance Commissioners' Insurance Data Security Model Law to establish insurance data security standards for Hawaii insurance licensees.

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

JUSTIFICATION SHEET

DEPARTMENT: Commerce and Consumer Affairs

TITLE: A BILL FOR AN ACT RELATING TO INSURANCE DATA SECURITY.

PURPOSE: To adopt the National Conference of Insurance Commissioners' (NAIC) Insurance Data Security Model Law to establish insurance data security standards for Hawaii insurance licensees.

MEANS: Add a new article to chapter 431, Hawaii Revised Statutes (HRS), and amend section 431:19-115(a), HRS.

JUSTIFICATION: The NAIC adopted the Data Security Model Law in 2017 to strengthen existing data privacy and consumer breach notification obligations of insurance licensees. The NAIC strongly encourages that states adopt this model law by 2022 or otherwise risk federal preemption of state laws in this area.

Impact on the public: None.

Impact on the department and other agencies:  
This bill will help the Department of Commerce and Consumer Affairs promote and enhance insurance data privacy and consumer breach notifications.

GENERAL FUNDS: None.

OTHER FUNDS: None.

PPBS PROGRAM DESIGNATION: CCA-106.

OTHER AFFECTED AGENCIES: None.



EFFECTIVE DATE: Upon approval; provided that licensees shall have one year from the effective date of this bill to implement sections 431:A-B through 431:A-I in section 1 of this bill, except that licensees shall have two years from the effective date of this bill to implement section 431:A-F in section 1 of this bill.