

2020 Regular Session

HOUSE BILL NO. 614

BY REPRESENTATIVE SEABAUGH

INSURANCE: Provides relative to data security for persons regulated by the commissioner of insurance

1 AN ACT

2 To amend and reenact R.S. 44:4.1(B)(11) and to enact Chapter 21 of Title 22 of the
3 Louisiana Revised Statutes of 1950, to be comprised of R.S. 22:2501 through 2511,
4 relative to data security for persons regulated by the commissioner of insurance; to
5 define key terms; to require licensees to maintain an information security program;
6 to provide for the investigation of data security breaches; to require notification of
7 data security breaches; to provide for the confidentiality of certain information; to
8 authorize penalties for violations; to provide for defenses; to establish a public
9 records exception; to provide for effectiveness; and to provide for related matters.

10 Be it enacted by the Legislature of Louisiana:

11 Section 1. Chapter 21 of Title 22 of the Louisiana Revised Statutes of 1950,
12 comprised of R.S. 22:2501 through 2511, is hereby enacted to read as follows:

13 CHAPTER 21. INSURANCE DATA SECURITY

14 §2501. Short title

15 This Chapter shall be known and may be cited as the "Insurance Data
16 Security Law".

17 §2502. Purpose and intent

18 A. This Chapter establishes the exclusive standards for this state applicable
19 to licensees for data security, the investigation of a cybersecurity event, and
20 notification to the commissioner.

1 B. This Chapter shall not be construed to create or imply a private cause of
2 action for violation of its provisions nor shall it be construed to curtail a private
3 cause of action that would otherwise exist in the absence of this Chapter.

4 §2503. Definitions

5 As used in this Chapter, the following definitions apply:

6 (1) "Authorized individual" means a natural person known to and screened
7 by a licensee and determined to be necessary and appropriate to have access to the
8 nonpublic information held by a licensee and its information systems.

9 (2) "Consumer" means a natural person who is a resident of this state and
10 whose nonpublic information is in a licensee's possession, custody, or control.

11 (3)(a) "Cybersecurity event" means an event resulting in unauthorized access
12 to or disruption or misuse of an information system or nonpublic information stored
13 on an information system.

14 (b) "Cybersecurity event" shall not include either of the following:

15 (i) The unauthorized acquisition of encrypted nonpublic information if the
16 encryption, process, or key is not also acquired, released, or used without
17 authorization.

18 (ii) An event with regard to which the licensee has determined that the
19 nonpublic information accessed by an unauthorized person has not been used or
20 released and has been returned or destroyed.

21 (4) "Encrypted" means the transformation of data into a form that has a low
22 probability of assigning meaning without the use of a protective process or key.

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

26 (6) "Information system" means a discrete set of electronic information
27 resources organized for the collection, processing, maintenance, use, sharing,
28 dissemination, or disposition of electronic nonpublic information. "Information
29 system" shall include any specialized system such as industrial or process controls

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

3 (7)(a) "Licensee" means any person licensed, authorized to operate, or
4 registered or required to be licensed, authorized, or registered pursuant to the
5 insurance laws of this state.

6 (b) "Licensee" shall not include either of the following:

7 (i) A purchasing group or a risk retention group chartered and licensed in a
8 state other than this state.

9 (ii) A person that is acting as an assuming insurer that is domiciled in
10 another state or jurisdiction.

11 (8) "Multi-factor authentication" means authentication through verification
12 of at least two of the following types of authentication factors:

13 (a) Knowledge factors, such as a password.

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

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

16 (9) "Nonpublic information" means electronic information that is not
17 publicly available information and is any of the following:

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

21 (i) Social Security number.

22 (ii) Driver's license number or nondriver identification card number.

23 (iii) Financial account number or credit or debit card number.

24 (iv) Any security code, access code, or password that would permit access
25 to a consumer's financial account.

26 (v) Biometric records.

27 (b) Any information or data, except age or gender, in any form or medium
28 created by or derived from a healthcare provider or a consumer, that can be used to
29 identify a particular consumer, and that relates to any of the following:

1 (i) The past, present, or future physical, mental, or behavioral health or
2 condition of any consumer.

3 (ii) The provision of health care to any consumer.

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

5 (10) "Person" means any natural person or any nongovernmental juridical
6 person.

7 (11) "Publicly available information" means any information that a licensee
8 reasonably believes is lawfully made available to the general public when all of the
9 following occur:

10 (a) The information is available to the general public from any of the
11 following sources:

12 (i) Federal, state, or local government records.

13 (ii) Widely distributed media.

14 (iii) Disclosures to the general public required to be made by federal, state,
15 or local law.

16 (b) A licensee has a reasonable basis to believe that information is lawfully
17 made available to the general public if the licensee has taken steps to determine all
18 of the following:

19 (i) That the information is of a type that is available to the general public.

20 (ii) That a consumer who can direct that the information not be made
21 available to the general public has not done so.

22 (12) "Risk assessment" means the risk assessment that each licensee is
23 required to conduct pursuant to R.S. 22:2504(C).

24 (13) "Third-party service provider" means a person, not otherwise defined
25 as a licensee, who contracts with a licensee to maintain, process, store, or otherwise
26 have access to nonpublic information through its provision of services to the
27 licensee.

1 §2504. Information security program

2 A. A licensee shall develop, implement, and maintain a comprehensive,
3 written information security program which satisfies all of the following criteria:

4 (1) Is based on the licensee's risk assessment.

5 (2) Contains administrative, technical, and physical safeguards for the
6 protection of nonpublic information and the licensee's information system.

7 (3) Is commensurate with all of the following:

8 (i) Size and complexity of the licensee.

9 (ii) Nature and scope of the licensee's activities including its use of
10 third-party service providers.

11 (iii) Sensitivity of the nonpublic information used by the licensee or in the
12 licensee's possession, custody, or control.

13 B. A licensee's information security program shall be designed to do all of
14 the following:

15 (1) Protect the security and confidentiality of nonpublic information and the
16 security of the information system.

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

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

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

23 C. A licensee shall conduct a risk assessment by doing all of the following:

24 (1) Designate one or more employees, an affiliate, or an outside vendor to
25 act on behalf of the licensee and to be responsible for the information security
26 program.

27 (2) Identify reasonably foreseeable internal or external threats that could
28 result in unauthorized access, transmission, disclosure, misuse, alteration, or
29 destruction of nonpublic information, including the security of information systems

1 and nonpublic information that are accessible to or held by third-party service
2 providers.

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

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

8 (a) Employee training and management.

9 (b) Information systems, including network and software design, as well as
10 information classification, governance, processing, storage, transmission, and
11 disposal.

12 (c) Detecting, preventing, and responding to attacks, intrusions, or other
13 systems failures.

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

17 D. Based on the licensee's risk assessment, a licensee shall do all of the
18 following:

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

24 (2) Implement all of the following security measures that the licensee
25 determines are appropriate:

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

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

4 (c) Restrict physical access to nonpublic information to authorized
5 individuals.

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

10 (e) Adopt secure development practices for in-house developed applications
11 used by the licensee and procedures for evaluating, assessing, or testing the security
12 of externally developed applications used by the licensee.

13 (f) Modify the information system in accordance with the licensee's
14 information security program.

15 (g) Use effective controls, which may include multifactor authentication
16 procedures for any individual accessing nonpublic information.

17 (h) Regularly test and monitor systems and procedures to detect actual and
18 attempted attacks on or intrusions into information systems.

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

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

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

28 (3) Include cybersecurity risks in the licensee's enterprise risk management
29 process.

1 (4) Stay informed regarding emerging threats or vulnerabilities.

2 (5) Use reasonable security measures when sharing information relative to
3 the character of the sharing and the type of information shared.

4 (6) Provide its personnel with cybersecurity awareness training that reflects
5 current risks identified by the licensee in the risk assessment.

6 E. If a licensee has a board of directors, the board or an appropriate
7 committee of the board shall, at a minimum, require a licensee's executive
8 management or its delegates to do all of the following:

9 (1) Develop, implement, and maintain the licensee's information security
10 program.

11 (2) Report in writing, at least annually, all of the following information:

12 (a) The overall status of the information security program and the licensee's
13 compliance with this Chapter.

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

19 (3) If executive management delegates any of the responsibilities provided
20 for in this Section, management shall oversee the development, implementation, and
21 maintenance of the licensee's information security program prepared by the delegates
22 and shall receive a report from the delegates complying with the requirements of the
23 report to the board of directors above.

24 F. With regard to third-party service providers, a licensee shall do all of the
25 following:

26 (1) Exercise due diligence in selecting a third-party service provider.

27 (2) Require third-party service providers to implement appropriate
28 administrative, technical, and physical measures to protect and secure the

1 information systems and nonpublic information that are accessible to or held by the
2 third-party service provider.

3 G. A licensee shall monitor, evaluate, and adjust, as appropriate, the
4 information security program consistent with any relevant changes in technology, the
5 sensitivity of its nonpublic information, internal or external threats to information,
6 and the licensee's own changing business arrangements, including but not limited to
7 mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and
8 changes to information systems.

9 H.(1) As part of its information security program, each licensee shall
10 establish a written incident response plan designed to promptly respond to, and
11 recover from, any cybersecurity event that compromises the confidentiality,
12 integrity, or availability of nonpublic information in its possession, the licensee's
13 information systems, or the continuing functionality of any aspect of the licensee's
14 business or operations.

15 (2) The incident response plan shall address all of the following:

16 (a) The internal process for responding to a cybersecurity event.

17 (b) The goals of the incident response plan.

18 (c) The definition of clear roles, responsibilities, and levels of
19 decisionmaking authority.

20 (d) External and internal communications and information sharing.

21 (e) Identification of requirements for the remediation of any identified
22 weaknesses in information systems and associated controls.

23 (f) Documentation and reporting regarding cybersecurity events and related
24 incident response activities.

25 (g) The evaluation and revision of the incident response plan, as necessary,
26 following a cybersecurity event.

27 I.(1) Annually, each insurer domiciled in this state shall submit to the
28 commissioner a written statement by February 15, certifying that the insurer is in
29 compliance with the requirements set forth in R.S. 22:2504.

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

3 (3) To the extent an insurer identifies areas, systems, or processes that
4 require material improvement, update, or redesign, the insurer shall document the
5 identification and the remediation efforts planned and underway to address the areas,
6 systems, or processes. The documentation shall be made available for inspection by
7 the commissioner.

8 §2505. Investigation of a cybersecurity event

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

12 B. During the investigation, the licensee, or an outside vendor or service
13 provider designated to act on behalf of the licensee, shall do all of the following to
14 the extent possible:

15 (1) Determine whether a cybersecurity event has occurred.

16 (2) Assess the nature and scope of the cybersecurity event.

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

19 (4) Undertake reasonable measures to restore the security of the information
20 systems compromised in the cybersecurity event in order to prevent further
21 unauthorized acquisition, release, or use of nonpublic information in the licensee's
22 possession, custody, or control.

23 C. If a licensee learns that a cybersecurity event has or may have occurred
24 in a system maintained by a third-party service provider, the licensee shall make
25 reasonable efforts to complete the steps required pursuant to Subsection B of this
26 Section or make reasonable efforts to confirm and document that the third-party
27 service provider has completed those steps.

1 D. The licensee shall maintain records concerning all cybersecurity events
2 for a period of at least five years from the date of the cybersecurity event and shall
3 produce those records upon demand of the commissioner.

4 §2506. Notification of a cybersecurity event

5 A. A licensee shall notify the commissioner without unreasonable delay but
6 in no event later than three business days from a determination that a cybersecurity
7 event involving nonpublic information that is in the possession of the licensee has
8 occurred when either of the following criteria has been met:

9 (1) This state is the licensee's state of domicile, in the case of an insurer, or
10 this state is the licensee's home state, in the case of a producer, an adjuster, or public
11 adjuster as those terms are defined in R.S. 22:1542, 1661, or 1692, and the
12 cybersecurity event has reasonable likelihood of materially harming either of the
13 following:

14 (a) Any consumer residing in this state.

15 (b) Any material part of the normal operations of the licensee.

16 (2) A licensee reasonably believes that the nonpublic information involved
17 is for two hundred fifty or more consumers residing in this state and that either of the
18 following has occurred:

19 (a) A cybersecurity event affecting the licensee of which notice is required
20 to be provided to any government body, self-regulatory agency, or any other
21 supervisory body pursuant to any state or federal law.

22 (b) A cybersecurity event that has a reasonable likelihood of materially
23 harming any of the following:

24 (i) Any consumer residing in this state.

25 (ii) Any material part of the normal operations of the licensee.

26 B.(1) The licensee shall have a continuing obligation to update and
27 supplement initial and subsequent notifications to the commissioner regarding
28 material changes to previously provided information relative to the cybersecurity
29 event.

1 (2) The licensee making the notification required in Subsection A of this
2 Section shall provide as much of the following information as possible in electronic
3 form as directed by the commissioner:

4 (a) Date of the cybersecurity event.

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

8 (c) How the cybersecurity event was discovered.

9 (d) Whether any lost, stolen, or breached information has been recovered
10 and, if so, how recovery was accomplished.

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

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

15 (g)(i) Description of the specific types of information acquired without
16 authorization.

17 (ii) For the purposes of this Subparagraph, "specific types of information"
18 means particular data elements including but not limited to types of medical
19 information, types of financial information, or types of information allowing
20 identification of the consumer.

21 (h) The period during which the cybersecurity event compromised the
22 information system.

23 (i)(i) The total number of consumers in this state affected by the
24 cybersecurity event.

25 (ii) The licensee shall provide the best estimate in the initial report to the
26 commissioner and update this estimate with each subsequent report to the
27 commissioner pursuant to this Section.

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

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

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

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

11 C. A licensee shall comply with the Database Security Breach Notification
12 Law, R.S. 51:3071 et seq., as applicable, and shall provide to the commissioner a
13 copy of the notice sent to consumers if the licensee is required to notify the
14 commissioner pursuant to Subsection A of this Section.

15 D.(1) In the case of a cybersecurity event in a system maintained by a
16 third-party service provider of which the licensee has become aware, all of the
17 following shall apply:

18 (a) The licensee shall treat the cybersecurity event as it would pursuant to
19 Subsection A of this Section, unless the third-party service provider gives the notice
20 required in Subsection A of this Section.

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

25 (2) Nothing in this Chapter shall be construed to prevent or abrogate an
26 agreement between a licensee and another licensee, a third-party service provider,
27 or any other party to fulfill any of the investigation requirements pursuant to R.S.
28 22:2505 or notice requirements pursuant to this Section.

1 E.(1)(a) In the case of a cybersecurity event involving nonpublic information
2 used by a licensee acting as an assuming insurer or in the possession, custody, or
3 control of a licensee acting as an assuming insurer and that does not have a direct
4 contractual relationship with the affected consumers, the assuming insurer shall
5 notify its affected ceding insurers and the commissioner of its state of domicile
6 within three business days of making the determination that a cybersecurity event has
7 occurred.

8 (b) The ceding insurers that have a direct contractual relationship with
9 affected consumers shall fulfill the consumer notification requirements pursuant to
10 the Database Security Breach Notification Law and any other notification
11 requirements relating to a cybersecurity event pursuant to this Section.

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

18 (b) The ceding insurers that have a direct contractual relationship with
19 affected consumers shall fulfill the consumer notification requirements pursuant to
20 the Database Security Breach Notification Law and any other notification
21 requirements relating to a cybersecurity event pursuant to this Section.

22 F. In the case of a cybersecurity event involving nonpublic information that
23 is in the possession, custody, or control of a licensee that is an insurer or its
24 third-party service provider for which a consumer accessed the insurer's services
25 through an independent insurance producer and for which consumer notice is
26 required by the Database Security Breach Notification Law, the insurer shall notify
27 the producers of record of all affected consumers of the cybersecurity event no later
28 than the time at which notice is provided to the affected consumers. The insurer
29 shall be excused from this obligation for any producers who are not authorized by

1 law or contract to sell, solicit, or negotiate on behalf of the insurer, and in those
2 instances in which the insurer does not have the current producer of record
3 information for an individual consumer.

4 §2507. Powers of the commissioner

5 A. The commissioner may examine and investigate into the affairs of any
6 licensee to determine whether the licensee has been or is engaged in any conduct in
7 violation of this Chapter. This power is in addition to the powers which the
8 commissioner has pursuant to R.S. 22:1981, 1983, and 1984. Any investigation or
9 examination shall be conducted pursuant to R.S. 22:1983 and 1984.

10 B. Whenever the commissioner has reason to believe that a licensee has been
11 or is engaged in conduct in this state which violates this Chapter, the commissioner
12 may take any action that is necessary or appropriate to enforce the provisions of this
13 Chapter.

14 §2508. Confidentiality

15 A. Any documents, materials, or other information in the control or
16 possession of the commissioner that are furnished by a licensee or an employee or
17 agent acting on behalf of a licensee pursuant to R.S. 22:2504 or 2506 or that are
18 obtained by the commissioner in an investigation or examination pursuant to R.S.
19 22:2507 shall be confidential by law and privileged, shall not be subject to release
20 pursuant to the Public Records Law, R.S. 44:1 et seq., shall not be subject to
21 subpoena, and shall not be subject to discovery or admissible in evidence in any
22 private civil action. However, the commissioner may use the documents, materials,
23 or other information in the furtherance of any regulatory or legal action brought as
24 a part of the commissioner's duties. The commissioner shall not otherwise make the
25 documents, materials, or other information public.

26 B. Neither the commissioner nor any person who received documents,
27 materials, or other information while acting pursuant to the authority of the
28 commissioner shall testify in any private civil action concerning any confidential
29 documents, materials, or information subject to Subsection A of this Section.

1 C. In order to assist in the performance of the commissioner's duties pursuant
2 to this Chapter, the commissioner may do any of the following:

3 (1) Share documents, materials, or other information, including the
4 confidential and privileged documents, materials, or information subject to
5 Subsection A of this Section, with other state, federal, and international regulatory
6 agencies, with the National Association of Insurance Commissioners, its affiliates,
7 or subsidiaries, and with state, federal, and international law enforcement authorities,
8 if the recipient agrees in writing to maintain the confidentiality and privileged status
9 of the document, material, or other information.

10 (2)(a) Receive documents, materials, or information, including otherwise
11 confidential and privileged documents, materials, or information, from the National
12 Association of Insurance Commissioners, its affiliates, or subsidiaries and from
13 regulatory and law enforcement officials of other foreign or domestic jurisdictions.

14 (b) The commissioner shall maintain as confidential or privileged any
15 document, material, or information received with notice or the understanding that the
16 document, material, or information is confidential or privileged pursuant to the laws
17 of the jurisdiction that is the source of the document, material, or information.

18 (3) Share documents, materials, or other information subject to Subsection
19 A of this Section with a third-party consultant or vendor if the consultant agrees in
20 writing to maintain the confidentiality and privileged status of the document,
21 material, or other information.

22 (4) Enter into agreements governing the sharing and use of information
23 consistent with this Subsection.

24 D. No waiver of any applicable privilege or claim of confidentiality in the
25 documents, materials, or information shall occur as a result of disclosure to the
26 commissioner pursuant to this Section or as a result of sharing pursuant to
27 Subsection C of this Section.

28 E. Nothing in this Chapter shall be construed to prohibit the commissioner
29 from releasing final, adjudicated actions that are open to public inspection pursuant

1 to the Public Records Law or to a database or other clearinghouse service maintained
2 by the National Association of Insurance Commissioners, its affiliates, or
3 subsidiaries.

4 F. Documents, materials, or other information in the possession or control
5 of the National Association of Insurance Commissioners (NAIC) or a third-party
6 consultant or vendor pursuant to this Chapter shall be confidential by law and
7 privileged, shall not be subject to release pursuant to the Public Records Law, R.S.
8 44:1 et seq., shall not be subject to subpoena, and shall not be subject to discovery
9 or admissible in evidence in any private civil action.

10 §2509. Exemptions

11 A. A licensee shall be exempt from the provisions of R.S. 22:2504 if the
12 licensee meets any of the following criteria:

13 (1) Having fewer than twenty-five employees.

14 (2) Less than five million dollars in gross annual revenue.

15 (3) Less than ten million dollars in year-end total assets.

16 (4) Being subject to the Health Insurance Portability and Accountability Act,
17 Pub.L. 104-191, 110 Stat. 1936, and doing all of the following:

18 (a) Establishing and maintaining an information security program pursuant
19 to any statutes, rules, regulations, procedures, or guidelines established pursuant to
20 the Health Insurance Portability and Accountability Act.

21 (b) Complying with and submitting a written statement certifying
22 compliance with the information security program established and maintained
23 pursuant to Subparagraph (a) of this Paragraph.

24 (3) Being an employee, agent, representative, or designee of a licensee, who
25 is also a licensee, to the extent that the employee, agent, representative, or designee
26 is covered by the information security program of the other licensee.

27 (4) Being affiliated with a depository institution subject to the Interagency
28 Guidelines Establishing Information Security Standards pursuant to the Gramm-
29 Leach-Bliley Act, 15 U.S.C. 6801 and 6805, and doing all of the following:

1 (a) Establishing and maintaining an information security program pursuant
2 to any statutes, rules, regulations, procedures, or guidelines established pursuant to
3 the Gramm-Leach-Bliley Act.

4 (b) Complying with and submitting a written statement certifying
5 compliance with the information security program established and maintained
6 pursuant to Subparagraph (a) of this Paragraph.

7 (5) Being subject to another jurisdiction approved by the commissioner and
8 doing all of the following:

9 (a) Establishing and maintaining an information security program pursuant
10 to such statutes, rules, regulations, procedures, or guidelines established by another
11 jurisdiction.

12 (b) Complying with and submitting a written statement certifying its
13 compliance with the information security program established and maintained
14 pursuant to Subparagraph (a) of this Paragraph.

15 B. In the event that a licensee ceases to qualify for an exemption pursuant
16 to Subsection A of this Section, the licensee shall have one hundred eighty days to
17 comply with the provisions of this Chapter.

18 C. A licensee that is subject to R.S. 51:3076 shall be exempt from the
19 provisions of R.S. 22:2506 if the licensee does all of the following:

20 (1) Notifies affected consumers of cybersecurity events relating to the
21 licensee's insurance business in a manner consistent with the requirements of the
22 Gramm-Leach-Bliley Act.

23 (2) Notifies the commissioner of cybersecurity events relating to the
24 licensee's insurance business in a manner consistent with and at the same time as the
25 notice the licensee gives to federal regulatory authorities.

26 §2510. Penalties

27 In the case of a violation of this Chapter, the commissioner may impose a
28 penalty pursuant to R.S. 22:18.

DIGEST

The digest printed below was prepared by House Legislative Services. It constitutes no part of the legislative instrument. The keyword, one-liner, abstract, and digest do not constitute part of the law or proof or indicia of legislative intent. [R.S. 1:13(B) and 24:177(E)]

HB 614 Engrossed

2020 Regular Session

Seabaugh

Abstract: Establishes the "Insurance Data Security Law".

Proposed law enacts the Insurance Data Security Law to establish standards for data security and for the investigation of and notification to the commissioner of a cybersecurity event applicable to licensees of the Department of Insurance.

Proposed law defines "authorized individual", "consumer", "cybersecurity event", "encrypted", "information security program", "information system", "licensee", "multi-factor authentication", "nonpublic information", "person", "publicly available information", "risk assessment", and "third-party service provider".

Proposed law requires a licensee to develop, implement, and maintain a comprehensive, written information security program which satisfies the criteria required by proposed law and does all of the following:

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

Proposed law requires a licensee to conduct a risk assessment that meets the criteria specified in proposed law, design an information security program to mitigate the identified risks, and implement appropriate security measures.

Proposed law provides for the duties of the licensee's board of directors.

Proposed law provides for the duties of a licensee with regard to third-party service providers.

Proposed law requires the licensee to 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.

Proposed law requires each licensee to 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 and establishes the minimum requirements of the response plan.

Proposed law requires a licensee which learns that a cybersecurity event has or may have occurred, or an outside vendor or service provider designated to act on behalf of the licensee,

to conduct a prompt investigation and provides for the requirements of the investigation and subsequent documentation.

Proposed law provides for the notification duties of a licensee once there is a determination that a cybersecurity event has occurred.

Proposed law authorizes the commissioner to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any violation of proposed law and to take any action that is necessary or appropriate to enforce the provisions of proposed law whenever the commissioner has reason to believe that a licensee has been or is engaged in a violation of proposed law.

Proposed law provides for the confidentiality of any documents, materials, or other information in the control or possession of the commissioner that are furnished by a licensee or an employee or agent acting on behalf of a licensee pursuant to proposed law, including an exemption to the Public Records Law and prohibits the commissioner from making such information public.

Proposed law requiring a licensee to develop, implement, and maintain a comprehensive, written information security program does not apply to a licensee who is any of the following:

- (1) Having fewer than 25 employees.
- (2) Have less than \$5 million in gross annual revenue.
- (3) Have less than \$10 million in year-end total assets.
- (4) Establishing and maintaining an information security program pursuant to the federal Health Insurance Portability and Accountability Act.
- (5) An employee, agent, representative, or designee of a licensee, who is also a licensee, to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.
- (6) Notify affected consumers and the commissioner consistent with the requirements of the Gramm-Leach-Bliley Act.

Proposed law authorizes the commissioner to do any of the following in the event of a violation of proposed law:

- (1) Suspend, revoke, or refuse to renew the certificate of authority or license of any insurer, person, or entity.
- (2) Levy a fine not to exceed \$1,000 for each violation per insurer, person, or entity, up to \$100,000 aggregate for all violations in a calendar year per insurer, person, or entity.
- (3) Order any insurer, person, or entity to cease and desist any action that violates any provision of proposed law.

Proposed law provides that the provisions of R.S. 22:2504(F) shall become effective on Aug. 1, 2022, the provisions of R.S. 22:250 shall become effective on Aug. 1, 2021, and Sections 1, 2, 3, and 4 shall become effective on Aug. 1, 2020.

(Amends R.S. 44:4.1(B)(11); Adds R.S. 22:2501-2511)

Summary of Amendments Adopted by House

The Committee Amendments Proposed by House Committee on Insurance to the original bill:

1. Remove provision of proposed law which states the purpose and intent of proposed law and replace it with a provision which states that proposed law establishes exclusive standards for La. which are applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the commissioner.
2. Specify that references in definitions of "cybersecurity event" and "information system" regarding information means nonpublic information.
3. Change a provision in the list of exclusions set forth in the definition of a "licensee" from a licensee acting as an assuming insurer that is domiciled in another state or jurisdiction to a person acting as such an assuming insurer.
4. Clarify that the definition of "nonpublic information" refers to electronic information.
5. Remove a provision of proposed law that defines "nonpublic information" as business-related information of a licensee that would cause an adverse impact to the business, operations, or security of the licensee if the information were to be tampered with or be disclosed, accessed, or used without authorization.
6. Clarify that the reference to an account number in the list of identifying information contained in the definition of "nonpublic information" is a financial account number.
7. Clarify that information or data created or derived from a healthcare provider or consumer be information that identifies a particular consumer in order for it to be identifying information for the purposes of defining "nonpublic information."
8. Add that a licensee who learns about a cybersecurity event relative to a third-party service provider's system make a reasonable effort to complete the steps required by proposed law or make a reasonable effort to confirm and document that the third-party service provider has completed such steps.
9. Change notice requirements from requiring that a licensee notify the commissioner of a cybersecurity event as promptly as possible but no later than seventy-two hours to requiring that a licensee furnish such notice without unreasonable delay but no later than three business days, and change subsequent notice requirement references of seventy-two hours to three business days.
10. Clarify that the notice requirement refers to a cybersecurity event involving nonpublic information in the possession of the licensee.
11. Add adjusters and public adjusters as defined in present law, R.S. 22:1661 and 1692, to the notification criterion regarding the licensee's domicile or home state.
12. Add to the criterion regarding the licensee's domicile or home state that the cybersecurity event has reasonable likelihood of materially harming either any consumer residing in this state or any material part of the normal operation of the licensee.
13. Clarify that subsequent notice requirements apply to material changes to previously provided information relative to the cybersecurity event.

14. Clarify that the requirements regarding what information be provided to the commissioner regarding the cybersecurity event be provided when making notice as required by proposed law.
15. Add an exception to the requirement that licensees give notice of a cybersecurity event when a system is maintained by a third-party service provider when the third-party service provider has already given notice as required by proposed law.
16. Add to the provision requiring notice when a cybersecurity event involves information accessed by the consumer through an independent insurance producer that such notice be required when it is required by the Database Security Breach Notification Law.
17. Change the requirement for when a cybersecurity event involves information accessed by the consumer through an independent insurance producer from as soon as practicable as directed by the commissioner to no later than the time at which notice is provided to the affected consumers.
18. Add to the provision requiring notice when a cybersecurity event involves information accessed by the consumer through an independent insurance producer that an insurer is excused from this obligation for any producers who are not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer.
19. Add to Public Records Law exception that the commissioner cannot otherwise make the documents, materials, or other information public.
20. Add a provision that excludes documents, materials, or other information in the control of the NAIC or a third-party from the Public Records Law.
21. Change the provision that a licensee is excluded from the information security program if the licensee has fewer than ten employees to if the licensee has fewer than twenty-five employees and remove the inclusion of independent contractors.
22. Add to the list of criteria for the exclusion of a licensee from the information security program that the licensee has less than five million dollars in gross annual revenue and less than ten million dollars in year-end total assets.
23. Add to the list of criteria for the exclusion of a licensee from the information security program if the licensee is subject to the Gramm-Leach-Bliley Act and meet the requirements of the act.
24. Add to the list of criteria for the exclusion of a licensee from the information security program if the licensee is subject to present law and notify affected consumers and the commissioner consistent with the requirements of the Gramm-Leach-Bliley Act.
25. Add that a licensee who satisfies the provisions of proposed law may assert a defense to any cause of action arising in tort and alleging the failure to implement reasonable information security controls resulted in a data breach of nonpublic information.
26. Add that the provisions of R.S. 22:2504(F) shall become effective on Aug. 1, 2022, the provisions of R.S. 22:250 shall become effective on Aug. 1, 2021, and Sections 1, 2, 3, and 4 shall become effective on Aug. 1, 2020.