

STATE OF RHODE ISLAND

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2022

A N A C T

RELATING TO INSURANCE -- INSURANCE DATA SECURITY ACT

Introduced By: Representatives Kennedy, Azzinaro, Edwards, Diaz, Phillips, Kazarian,
and Solomon

Date Introduced: March 03, 2022

Referred To: House Corporations

(Dept. of Business Regulation)

It is enacted by the General Assembly as follows:

1 SECTION 1. Title 27 of the General Laws entitled "INSURANCE" is hereby amended by
2 adding thereto the following chapter:

3 CHAPTER 1.3

4 INSURANCE DATA SECURITY ACT

5 **27-1.3-1. Title.**

6 This chapter shall be known and may be cited as the "Insurance Data Security Act."

7 **27-1.3-2. Purpose and intent.**

8 (a) The purpose and intent of this chapter is to establish standards for data security and
9 standards for the investigation of, and notification to the commissioner of, a cybersecurity event
10 applicable to licensees, as defined in § 27-1.3-3. Notwithstanding any other provision of law, this
11 chapter establishes the exclusive state standards applicable to licensees for data security, the
12 investigation of a cybersecurity event as defined in § 27-1.3-3, and notification to the
13 commissioner. These provisions do not affect a licensee's responsibility to notify consumers in
14 accordance with § 27-1.3-6(c).

15 (b) This chapter may not be construed to create or imply a private cause of action for
16 violation of its provisions nor may it be construed to curtail a private cause of action which would
17 otherwise exist in the absence of this chapter.

18 **27-1.3-3. Definitions.**

19 As used in this chapter, the following terms shall have the following meanings:

1 (1) "Authorized individual" means an individual known to and screened by the licensee
2 and determined to be necessary and appropriate to have access to the nonpublic information held
3 by the licensee and its information systems.

4 (2) "Commissioner" shall have the meaning established in § 42-14-5.

5 (3) "Consumer" means an individual, including, but not limited to, applicants,
6 policyholders, insureds, beneficiaries, claimants, and certificate holders who is a resident of this
7 state and whose nonpublic information is in a licensee's possession, custody or control.

8 (4) "Cybersecurity event" means an event resulting in unauthorized access to, disruption
9 or misuse of, an information system or nonpublic information stored on such information system.

10 (i) The term "cybersecurity event" does not include the unauthorized acquisition of
11 encrypted nonpublic information if the encryption, process or key is not also acquired, released or
12 used without authorization.

13 (ii) "Cybersecurity event" does not include an event with regard to which the licensee has
14 determined that the nonpublic information accessed by an unauthorized person has not been used
15 or released and has been returned or destroyed.

16 (5) "Department" means the department of business regulation, division of insurance.

17 (6) "Encrypted" means the transformation of data into a form which results in a low
18 probability of assigning meaning without the use of a protective process or key.

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

22 (8) "Information system" means a discrete set of electronic information resources
23 organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of
24 electronic information, as well as any specialized system such as industrial/process controls
25 systems, telephone switching and private branch exchange systems, and environmental control
26 systems.

27 (9) "Licensee" means any person licensed, authorized to operate, or registered, or required
28 to be licensed, authorized, or registered pursuant to the insurance laws of this state, but shall not
29 include a purchasing group or a risk retention group chartered and licensed in a state other than this
30 state or a licensee that is acting as an assuming insurer that is domiciled in another state or
31 jurisdiction.

32 (10) "Multi-factor authentication" means authentication through verification of at least two
33 (2) of the following types of authentication factors:

34 (i) Knowledge factors, such as a password; or

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

2 (iii) Inherence factors, such as a biometric characteristic.

3 (11) "Nonpublic information" means information that is not publicly available information
4 and is:

5 (i) Business related information of a licensee the tampering with which, or unauthorized
6 disclosure, access or use of which, would cause a material adverse impact to the business,
7 operations or security of the licensee;

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

11 (A) Social security number;

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

13 (C) Account number, credit or debit card number;

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

16 (E) Biometric records;

17 (iii) Any information or data, except age or gender, in any form or medium created by or
18 derived from a health care provider or a consumer and that relates to:

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

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

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

23 (12) "Person" means any individual or any non-governmental entity, including, but not
24 limited to, any non-governmental partnership, corporation, limited liability company, branch,
25 agency or association.

26 (13) "Publicly available information" means any information that a licensee has a
27 reasonable basis to believe is lawfully made available to the general public from: federal, state or
28 local government records; widely distributed media; or disclosures to the general public that are
29 required to be made by federal, state or local law:

30 (i) For the purposes of this definition, a licensee has a reasonable basis to believe that
31 information is lawfully made available to the general public if the licensee has taken steps to
32 determine:

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

34 (B) Whether a consumer can direct that the information not be made available to the general

1 public and the consumer has not done so.

2 (14) "Risk assessment" means the procedure that each licensee is required to complete
3 under § 27-1.3-4(c).

4 (15) "State" means the State of Rhode Island.

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

8 **27-1.3-4. Information security program.**

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

16 (b) Objectives of information security program. A licensee's information security program
17 shall be designed to:

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

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

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

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

26 (c) Risk assessment. The licensee shall:

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

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

33 (3) Assess the likelihood and potential damage of these threats, taking into consideration
34 the sensitivity of the nonpublic information;

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

4 (i) Employee training and management;

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

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

8 and

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

12 (d) Risk management. Based on its risk assessment, the licensee shall:

13 (1) Design its information security program to mitigate the identified risks, commensurate
14 with the size and complexity of the licensee's activities, including its use of third-party service
15 providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's
16 possession, custody or control;

17 (2) Determine which security measures listed below are appropriate and implement such
18 security measures:

19 (i) Place access controls on information systems, including controls to authenticate and
20 permit access only to authorized individuals to protect against the unauthorized acquisition of
21 nonpublic information;

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

25 (iii) Restrict access at physical locations containing nonpublic information only to
26 authorized individuals;

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

30 (v) Adopt secure development practices for in-house developed applications utilized by the
31 licensee and procedures for evaluating, assessing or testing the security of externally developed
32 applications utilized by the licensee;

33 (vi) Modify the information system in accordance with the licensee's information security
34 program;

1 (vii) Utilize effective controls, which may include multi-factor authentication procedures
2 for any individual accessing nonpublic information;

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

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

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

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

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

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

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

19 (e) Oversight by board of directors. If the licensee has a board of directors, the board or an
20 appropriate committee of the board shall, at a minimum:

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

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

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

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

31 (3) If executive management delegates any of its responsibilities pursuant to this section,
32 it shall oversee the development, implementation and maintenance of the licensee's information
33 security program prepared by the designee(s) and shall receive a report from the designee(s)
34 complying with the requirements of the report to the board of directors.

1 (f) Oversight of third-party service provider arrangements.

2 (1) A licensee shall exercise due diligence in selecting its third-party service provider; and

3 (2) A licensee shall take reasonable steps to request a third-party service provider to
4 implement appropriate administrative, technical, and physical measures to protect and secure the
5 information systems and nonpublic information that are accessible to, or held by, the third-party
6 service provider.

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

12 (h) Incident response plan:

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

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

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

20 (ii) The goals of the incident response plan;

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

22 (iv) External and internal communications and information sharing;

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

25 (vi) Documentation and reporting regarding cybersecurity events and related incident
26 response activities; and

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

29 (i) Annual certification to commissioner of domiciliary state. Annually, each insurer
30 domiciled in this state shall submit to the commissioner a written statement by February 15
31 certifying that the insurer is in compliance with the requirements set forth in this section. Each
32 insurer shall maintain for examination by the department all records, schedules and data supporting
33 this certificate for a period of five (5) years. To the extent an insurer has identified areas, systems
34 or processes that require material improvement, updating or redesign, the insurer shall document

1 the identification and the remedial efforts planned and underway to address such areas, systems or
2 processes. This documentation must be available for inspection by the commissioner.

3 **27-1.3-5. Investigation of a cybersecurity event.**

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

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

10 (1) Whether a cybersecurity event has occurred;

11 (2) Assess the nature and scope of the cybersecurity event;

12 (3) Identify any nonpublic information that may have been involved in the cybersecurity
13 event; and

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

17 (c) If the licensee learns that a cybersecurity event has or may have occurred in a system
18 maintained by a third-party service provider, and it has or may have impacted the licensee's
19 nonpublic information, the licensee shall make reasonable efforts to complete the steps set forth in
20 subsection (b) of this section or make reasonable efforts to confirm and document that the third-
21 party service provider has completed those steps.

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

25 **27-1.3-6. Notification of a cybersecurity event.**

26 (a) Notification to the commissioner. Each licensee shall notify the commissioner as
27 promptly as possible but in no event later than three (3) business days from a determination that a
28 cybersecurity event has occurred when either of the following criteria has been met:

29 (1) This state is the licensee's state of domicile, in the case of an insurer, or this state is the
30 licensee's home state, in the case of a producer, as those terms are defined in § 27-2.4-2; or

31 (2) The licensee reasonably believes that the nonpublic information involved affects two
32 hundred fifty (250) or more consumers residing in this state and that either of the following apply:

33 (i) A cybersecurity event impacting the licensee of which notice is required to be provided
34 to any government body, self-regulatory agency or any other supervisory body pursuant to any state

1 or federal law; or

2 (ii) A cybersecurity event that has a reasonable likelihood of materially harming:

3 (A) Any consumer residing in this state; or

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

5 (b) The licensee shall provide any information required by this section in electronic form

6 as directed by the commissioner. The licensee shall have a continuing obligation to update and

7 supplement initial and subsequent notifications to the commissioner concerning the cybersecurity

8 event. The licensee shall provide as much of the following information as possible:

9 (1) Date of the cybersecurity event;

10 (2) Description of how the information was exposed, lost, stolen, or breached, including

11 the specific roles and responsibilities of third-party service providers, if any;

12 (3) How the cybersecurity event was discovered;

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

14 this recovery was achieved;

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

16 (6) Whether the licensee has filed a police report or has notified any regulatory, government

17 or law enforcement agencies and, if so, when such notification was provided;

18 (7) Description of the specific types of information acquired without authorization.

19 Specific types of information consisting of particular data elements including, for example, types

20 of medical information, types of financial information or types of information allowing

21 identification of the consumer;

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

23 event;

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

25 licensee shall provide the best estimate in the initial report to the commissioner and update this

26 estimate with each subsequent report to the commissioner pursuant to this section;

27 (10) The results of any internal review identifying a lapse in either automated controls or

28 internal procedures, or confirming that all automated controls or internal procedures were followed;

29 (11) Description of efforts being undertaken to remediate the situation which permitted the

30 cybersecurity event to occur;

31 (12) A copy of the licensee's privacy policy and a statement outlining the steps the licensee

32 will take to investigate and notify consumers affected by the cybersecurity event; and

33 (13) Name of a contact person who is both familiar with the cybersecurity event and

34 authorized to act for the licensee.

1 (c) Notification to consumers. A licensee shall comply with chapter 49.3 of title 11, as
2 applicable, and provide a copy of the notice sent to consumers under that chapter to the
3 commissioner, when a licensee is required to notify the commissioner under subsection (a) of this
4 section.

5 (d) Notice regarding cybersecurity events of third-party service providers:

6 (1) In the case of a cybersecurity event involving a licensee's nonpublic information in a
7 system maintained by a third-party service provider, of which the licensee has become aware, the
8 licensee shall treat that event as it would under subsection (a) of this section;

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

12 (3) Nothing in this chapter shall prevent or abrogate an agreement between a licensee and
13 another licensee, a third-party service provider or any other party to fulfill any of the investigation
14 requirements imposed under § 27-1.3-5 or notice requirements imposed under this section.

15 (e) Notice regarding cybersecurity events of reinsurers to insurers:

16 (1)(i) In the case of a cybersecurity event involving nonpublic information that is used by
17 the licensee that is acting as an assuming insurer or in the possession, custody or control of a
18 licensee that is acting as an assuming insurer and that does not have a direct contractual relationship
19 with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the
20 commissioner of its state of domicile within seventy-two (72) hours of making the determination
21 that a cybersecurity event has occurred;

22 (ii) The ceding insurers that have a direct contractual relationship with affected consumers
23 shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11, the
24 "identity theft protection act of 2015", and any other notification requirements relating to a
25 cybersecurity event imposed under this section;

26 (2)(i) In the case of a cybersecurity event involving nonpublic information that is in the
27 possession, custody or control of a third-party service provider of a licensee that is an assuming
28 insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its
29 state of domicile within seventy-two (72) hours of receiving notice from its third-party service
30 provider that a cybersecurity event has occurred;

31 (ii) The ceding insurers that have a direct contractual relationship with affected consumers
32 shall fulfill the consumer notification requirements imposed under chapter 49.3 of title 11 and any
33 other notification requirements relating to a cybersecurity event imposed under this section.

34 (f) Notice regarding cybersecurity events of insurers to producers of record.

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

6 (2) The insurer is excused from this obligation for those instances in which it does not have
7 the current producer of record information for any individual consumer.

8 **27-1.3-7. Power of commissioner.**

9 (a) The commissioner shall have power to examine and investigate into the affairs of any
10 licensee to determine whether the licensee has been or is engaged in any conduct in violation of
11 this chapter. This power is in addition to the powers which the commissioner has pursuant to
12 chapter 13.1 of title 27 and any such investigation or examination shall be conducted pursuant to
13 chapter 13.1 of title 27.

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

17 **27-1.3-8. Confidentiality.**

18 (a) Any documents, materials or other information in the control or possession of the
19 department that are furnished by a licensee or an employee or agent thereof acting on behalf of a
20 licensee pursuant to §§ 27-1.3-4(i) and 27-1.3-6(b)(2), (3), (4), (5), (8), (10), and (11), or that are
21 obtained by the commissioner in an investigation or examination pursuant to § 27-1.3-7 shall be
22 confidential by law and privileged, shall not be subject to chapter 2 of title 38, shall not be subject
23 to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil
24 action; provided, however, the commissioner is authorized to use the documents, materials or other
25 information in the furtherance of any regulatory or legal action brought as a part of the
26 commissioner's duties.

27 (b) Neither the commissioner nor any person who received documents, materials or other
28 information while acting under the authority of the commissioner shall be permitted or required to
29 testify in any private civil action concerning any confidential documents, materials, or information
30 subject to subsection (a) of this section.

31 (c) In order to assist in the performance of the commissioner's duties under this chapter,
32 the commissioner:

33 (1) May share documents, materials or other information, including the confidential and
34 privileged documents, materials or information subject to subsection (a) of this section, with other

1 state, federal, and international regulatory agencies, with the National Association of Insurance
2 Commissioners, its affiliates or subsidiaries, and with state, federal, and international law
3 enforcement authorities; provided that, the recipient agrees in writing to maintain the
4 confidentiality and privileged status of the document, material or other information;

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

12 (3) May share documents, materials or other information subject to subsection (a) of this
13 section, with a third-party consultant or vendor provided the consultant agrees in writing to
14 maintain the confidentiality and privileged status of the document, material or other information;
15 and

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

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

21 (e) Nothing in this chapter shall prohibit the commissioner from releasing final, adjudicated
22 actions that are open to public inspection pursuant to chapter 2 of title 38 to a database or other
23 clearinghouse service maintained by the National Association of Insurance Commissioners, its
24 affiliates or subsidiaries.

25 **27-1.3-9. Exceptions.**

26 (a) The following exceptions shall apply to this chapter:

27 (1) A licensee with fewer than twenty-five (25) employees, including any independent
28 contractors with access to the licensee's nonpublic information; or

29 (2) A licensee with less than five million dollars (\$5,000,000) in gross annual revenue; or

30 (3) A licensee with less than ten million dollars (\$10,000,000) in assets, measured at the
31 end of the licensee's fiscal year, is exempt from § 27-1.3-4.

32 (4) A licensee subject to and in compliance with Pub. L. 104-191, 110 Stat. 1936, enacted
33 August 21, 1996 (Health Insurance Portability and Accountability Act) and related privacy, security
34 and breach notification regulations pursuant to 45 Code of Federal Regulations, Parts 160 and 164,

1 and Pub. L. 111-5, 123 Stat. 226, enacted February 17, 2009 (Health Information Technology) is
2 considered to meet the requirements of this chapter, other than the requirements of §§ 27-1.3-6(a)
3 and (b) regarding notification to the commissioner, if:

4 (i) The licensee maintains a program for information security and breach notification that
5 treats all nonpublic information relating to consumers in this state in the same manner as protected
6 health information;

7 (ii) The licensee annually submits to the commissioner a written statement certifying that
8 the licensee is in compliance with, the requirements of this subsection; and

9 (iii) The commissioner has not issued a determination finding that the applicable federal
10 regulations are materially less stringent than the requirements of this chapter.

11 (5) An employee, agent, representative or designee of a licensee, who is also a licensee, is
12 exempt from § 27-1.3-4 and need not develop its own information security program to the extent
13 that the employee, agent, representative or designee is covered by the information security program
14 of the other licensee.

15 (b) In the event that a licensee ceases to qualify for an exception, the licensee shall have
16 one hundred eighty (180) days to comply with this chapter.

17 **27-1.3-10. Penalties.**

18 In the case of a violation of this chapter, a licensee may be penalized in accordance with §
19 42-14-16.

20 **27-1.3-11. Severability.**

21 If any provision of this chapter or the application thereof to any person or circumstance is
22 for any reason held to be invalid, the remainder of the chapter and the application of such provision
23 to other persons or circumstances shall not be affected thereby.

24 SECTION 2. This act shall take effect on January 1, 2023.

=====
LC004692
=====

EXPLANATION
BY THE LEGISLATIVE COUNCIL
OF
A N A C T
RELATING TO INSURANCE -- INSURANCE DATA SECURITY ACT

1 This act is based on the National Association of Insurance Commissioners Model Act
2 regarding data security to establish standards for data security and standards for the investigation
3 of and notification to the commissioner of a cybersecurity event. This act would also provide that
4 all documents, materials or other information in the control of the department of business
5 regulation, division of insurance furnished by a licensee or that are obtained by the commissioner
6 in an investigation pursuant to § 27-1.3-7 shall be confidential and not subject to discovery and not
7 admissible in evidence in any private civil action.

8 This act would take effect on January 1, 2023.

=====
LC004692
=====