

IN THE HOUSE OF REPRESENTATIVES

HOUSE BILL NO. 147

BY BUSINESS COMMITTEE

AN ACT

1 RELATING TO THE INSURANCE DATA SECURITY ACT; AMENDING TITLE 41, IDAHO CODE,
2 BY THE ADDITION OF A NEW CHAPTER 66, TITLE 41, IDAHO CODE, TO PROVIDE A
3 SHORT TITLE, TO DEFINE TERMS, TO ESTABLISH PROVISIONS REGARDING AN IN-
4 FORMATION SECURITY PROGRAM, TO PROVIDE FOR INVESTIGATION OF A CYBERSE-
5 CURITY EVENT, TO PROVIDE FOR NOTICE OF A CYBERSECURITY EVENT, TO PROVIDE
6 THAT THE DIRECTOR OF THE DEPARTMENT OF INSURANCE WILL HAVE THE POWER TO
7 EXAMINE AND INVESTIGATE CERTAIN MATTERS, TO PROVIDE FOR CONFIDENTIAL-
8 ITY AND SHARING OF DOCUMENTS, MATERIALS, AND OTHER INFORMATION, TO PRO-
9 VIDE EXCEPTIONS, TO PROVIDE THAT THE CHAPTER DOES NOT CREATE A PRIVATE
10 CAUSE OF ACTION, TO PROVIDE FOR PENALTIES, TO ESTABLISH PROVISIONS RE-
11 GARDING EXCLUSIVE STATE STANDARDS AND REQUIREMENTS, TO PROVIDE RULE-
12 MAKING AUTHORITY, TO PROVIDE CONSIDERATIONS IN ADMINISTERING THE CHAP-
13 TER, TO ESTABLISH PROVISIONS REGARDING THE EFFECTIVE DATE OF THE CHAP-
14 TER, AND TO PROVIDE SEVERABILITY.
15

16 Be It Enacted by the Legislature of the State of Idaho:

17 SECTION 1. That Title 41, Idaho Code, be, and the same is hereby amended
18 by the addition thereto of a NEW CHAPTER, to be known and designated as Chap-
19 ter 66, Title 41, Idaho Code, and to read as follows:

20 CHAPTER 66
21 INSURANCE DATA SECURITY ACT

22 41-6601. SHORT TITLE. This chapter shall be known and may be cited as
23 the "Insurance Data Security Act."

24 41-6602. DEFINITIONS. As used in this chapter:

25 (1) "Authorized individual" means an individual known to and screened
26 by the licensee and determined to be necessary and appropriate to have access
27 to the nonpublic information held by the licensee and its information sys-
28 tems.

29 (2) "Consumer" means an individual, including but not limited to appli-
30 cants, policyholders, insureds, beneficiaries, claimants, and certificate
31 holders, who is a resident of this state and whose nonpublic information is
32 in a licensee's possession, custody, or control.

33 (3) "Cybersecurity event" means an event resulting in unauthorized ac-
34 cess to, disruption of, or misuse of an information system or nonpublic in-
35 formation stored on such information system. The term "cybersecurity event"
36 does not include:

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

1 (b) An event with regard to which the licensee has determined that the
2 nonpublic information accessed by an unauthorized person has not been
3 used or released and has been returned or destroyed.

4 (4) "Department" has the same meaning as provided in section 41-105,
5 Idaho Code.

6 (5) "Director" has the same meaning as provided in section 41-105,
7 Idaho Code.

8 (6) "Encrypted" means the transformation of data into a form that re-
9 sults in a low probability of assigning meaning without the use of a protec-
10 tive process or key.

11 (7) "Information security program" means the administrative, techni-
12 cal, and physical safeguards that a licensee uses to access, collect, dis-
13 tribute, process, protect, store, use, transmit, dispose of, or otherwise
14 handle nonpublic information.

15 (8) "Information system" means a discrete set of electronic informa-
16 tion resources organized for the collection, processing, maintenance, use,
17 sharing, dissemination, or disposition of electronic nonpublic informa-
18 tion, as well as any specialized system such as industrial/process controls
19 systems, telephone switching and private branch exchange systems, and envi-
20 ronmental control systems.

21 (9) "Licensee" means any person who is licensed, authorized to operate,
22 or registered, or who is required to be licensed, authorized, or registered,
23 pursuant to the insurance laws of this state but does not include a purchas-
24 ing group or a risk retention group chartered and licensed in a state other
25 than this state or a person that is acting as an assuming insurer domiciled in
26 another state or jurisdiction.

27 (10) "Multifactor authentication" means authentication through veri-
28 fication of at least two (2) of the following types of authentication fac-
29 tors:

30 (a) Knowledge factors, such as a password;

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

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

34 (11) "Nonpublic information" means electronic information that is not
35 publicly available information and is:

36 (a) Business-related information of a licensee, the tampering with
37 which, or unauthorized disclosure, access, or use of which, would cause
38 a material adverse impact to the business, operations, or security of
39 the licensee;

40 (b) Any information concerning a consumer that because of name, num-
41 ber, personal mark, or other identifier can be used to identify such
42 consumer, in combination with any one (1) or more of the following data
43 elements:

44 (i) Social security number;

45 (ii) Driver's license number or nondriver identification card
46 number;

47 (iii) Financial account number or credit or debit card number;

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

50 (v) Biometric records; or

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

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

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

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

9 (12) "Person" has the same meaning as provided in section 41-104, Idaho
 10 Code.

11 (13) "Publicly available information" means any information that a li-
 12 censee has a reasonable basis to believe is lawfully made available to the
 13 general public from: federal, state, or local government records; widely
 14 distributed media; or disclosures to the general public that are required to
 15 be made by federal, state, or local law. For the purposes of this defini-
 16 tion, a licensee has a reasonable basis to believe that information is law-
 17 fully made available to the general public if the licensee has taken steps to
 18 determine:

19 (a) That the information is of the type that is available to the general
 20 public; and

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

24 (14) "Risk assessment" means the risk assessment that each licensee is
 25 required to conduct under section 41-6603, Idaho Code.

26 (15) "State" means the state of Idaho or, when used in a context signify-
 27 ing a jurisdiction other than the state of Idaho, any state, district, terri-
 28 tory, commonwealth, or possession of the United States of America.

29 (16) "Third-party service provider" means a person, not otherwise de-
 30 fined as a licensee, that contracts with a licensee to maintain, process, or
 31 store nonpublic information or otherwise is permitted access to nonpublic
 32 information through its provision of services to the licensee.

33 41-6603. INFORMATION SECURITY PROGRAM. (1) Commensurate with the
 34 size and complexity of the licensee, the nature and scope of the licensee's
 35 activities, including its use of third-party service providers, and the
 36 sensitivity of the nonpublic information used by the licensee or in the
 37 licensee's possession, custody, or control, each licensee must develop, im-
 38 plement, and maintain a comprehensive written information security program
 39 based on the licensee's risk assessment that contains administrative, tech-
 40 nical, and physical safeguards for the protection of nonpublic information
 41 and the licensee's information system.

42 (2) A licensee must design its information security program to:

43 (a) Protect the security and confidentiality of nonpublic information
 44 and the security of the information system;

45 (b) Protect against reasonably foreseeable threats or hazards to the
 46 security or integrity of nonpublic information and the information sys-
 47 tem;

48 (c) Protect against unauthorized access to or use of nonpublic informa-
 49 tion and minimize the likelihood of harm to any consumer; and

1 (d) Define and periodically reevaluate a schedule for retention of non-
2 public information and a mechanism for its destruction when no longer
3 needed.

4 (3) The licensee must do all of the following:

5 (a) Designate one (1) or more employees, an affiliate, or an outside
6 vendor to act on behalf of the licensee who is responsible for the infor-
7 mation security program;

8 (b) Identify reasonably foreseeable internal or external threats that
9 could result in unauthorized access, transmission, disclosure, misuse,
10 alteration, or destruction of nonpublic information, including the se-
11 curity of information systems and nonpublic information that are acces-
12 sible to, or held by, third-party service providers;

13 (c) Assess the likelihood and potential damage of these threats, taking
14 into consideration the sensitivity of the nonpublic information;

15 (d) Assess the sufficiency of policies, procedures, information sys-
16 tems, and other safeguards in place to manage these threats, including
17 consideration of threats in each relevant area of the licensee's opera-
18 tions, including:

19 (i) Employee training and management;

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

23 (iii) Detecting, preventing, and responding to attacks, intru-
24 sions, or other systems failures; and

25 (e) Implement information safeguards to manage the threats identified
26 in its ongoing assessment and assess the effectiveness of the safe-
27 guards' key controls, systems, and procedures.

28 (4) Based on its risk assessment, the licensee must do the following:

29 (a) Design its information security program to mitigate the identified
30 risks, commensurate with the size and complexity of the licensee's ac-
31 tivities, including its use of third-party service providers, and the
32 sensitivity of the nonpublic information used by the licensee or in the
33 licensee's possession, custody, or control;

34 (b) Determine which of the following security measures are appropriate
35 and implement such security measures:

36 (i) Place access controls on information systems, including con-
37 trols to authenticate and permit access only to authorized indi-
38 viduals to protect against the unauthorized acquisition of non-
39 public information;

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

44 (iii) Restrict physical access to nonpublic information to autho-
45 rized individuals only;

46 (iv) Protect by encryption or other appropriate means all nonpub-
47 lic information while being transmitted over an external network
48 and all nonpublic information stored on a laptop computer or other
49 portable computing or storage device or media;

- 1 (v) Adopt secure development practices for in-house-developed
2 applications utilized by the licensee and procedures for evaluat-
3 ing, assessing, or testing the security of externally developed
4 applications utilized by the licensee;
- 5 (vi) Modify the information system in accordance with the li-
6 censee's information security program;
- 7 (vii) Utilize effective controls, which may include multifactor
8 authentication procedures for any employee or authorized individ-
9 ual accessing nonpublic information;
- 10 (viii) Regularly test and monitor systems and procedures to detect
11 actual and attempted attacks on, or intrusions into, information
12 systems;
- 13 (ix) Include audit trails within the information security program
14 designed to detect and respond to cybersecurity events and de-
15 signed to reconstruct material financial transactions sufficient
16 to support normal operations and obligations of the licensee;
- 17 (x) Implement measures to protect against destruction, loss,
18 or damage of nonpublic information due to environmental hazards,
19 such as fire and water damage or other catastrophes or technologi-
20 cal failures; and
- 21 (xi) Develop, implement, and maintain procedures for the secure
22 disposal of nonpublic information in any format;
- 23 (c) Include cybersecurity risks in the licensee's enterprise risk man-
24 agement process;
- 25 (d) Stay informed regarding emerging threats or vulnerabilities and
26 utilize reasonable security measures when sharing information relative
27 to the character of the sharing and the type of information shared; and
- 28 (e) Provide its personnel with cybersecurity awareness training that
29 is updated as necessary to reflect risks identified by the licensee in
30 the risk assessment.
- 31 (5) If the licensee has a board of directors, the board or an appropri-
32 ate committee of the board must, at a minimum, do the following:
- 33 (a) Require the licensee's executive management or its delegates to
34 develop, implement, and maintain the licensee's information security
35 program;
- 36 (b) Require the licensee's executive management or its delegates to re-
37 port in writing at least annually all of the following information:
- 38 (i) The overall status of the information security program and
39 the licensee's compliance with this chapter; and
- 40 (ii) Material matters related to the information security pro-
41 gram, addressing issues such as risk assessment, risk management
42 and control decisions, third-party service provider arrange-
43 ments, results of testing, cybersecurity events or violations and
44 management's responses thereto, and recommendations for changes
45 in the information security program; and
- 46 (c) If executive management delegates any of its responsibilities un-
47 der this section, it must oversee the development, implementation, and
48 maintenance of the licensee's information security program prepared by
49 the delegate and must receive a report from the delegate complying with
50 the requirements of the report to the board of directors.

1 (6) A licensee must exercise due diligence in selecting its third-party
2 service provider and must require a third-party service provider to imple-
3 ment appropriate administrative, technical, and physical measures to pro-
4 tect and secure the information systems and nonpublic information that are
5 accessible to, or held by, the third-party service provider. Nonpublic in-
6 formation is not accessible to, or held by, the third-party service provider
7 within the meaning of this section if it is encrypted and the associated pro-
8 tective process or key necessary to assign meaning to the nonpublic informa-
9 tion is not within the possession of the third-party service provider.

10 (7) The licensee must monitor, evaluate, and adjust, as appropriate,
11 the information security program consistent with all of the following:

12 (a) Any relevant changes in technology;

13 (b) The sensitivity of its nonpublic information;

14 (c) Internal or external threats to information; and

15 (d) The licensee's own changing business arrangements, such as mergers
16 and acquisitions, alliances and joint ventures, outsourcing arrange-
17 ments, and changes to information systems.

18 (8) As part of its information security program, each licensee must
19 establish a written incident response plan designed to promptly respond
20 to, and recover from, any cybersecurity event that compromises the con-
21 fidentiality, integrity, or availability of nonpublic information in its
22 possession, the licensee's information systems, or the continuing function-
23 ality of any aspect of the licensee's business or operations. Such incident
24 response plan must address the following areas:

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

26 (b) The goals of the incident response plan;

27 (c) The definition of clear roles, responsibilities, and levels of de-
28 cision-making authority;

29 (d) External and internal communications and information sharing;

30 (e) Identification of requirements for the remediation of any identi-
31 fied weaknesses in information systems and associated controls;

32 (f) Documentation and reporting regarding cybersecurity events and re-
33 lated incident response activities; and

34 (g) The evaluation and revision as necessary of the incident response
35 plan following a cybersecurity event.

36 (9) Annually, each insurer domiciled in this state must submit to the
37 director a written statement by April 15 certifying that the insurer is in
38 compliance with the requirements set forth in this section. Each insurer
39 must maintain for examination by the department all records, schedules,
40 and data supporting this certificate for a period of five (5) years. To the
41 extent an insurer has identified areas, systems, or processes that require
42 material improvement, updating, or redesign, the insurer must document the
43 identification and the remedial efforts planned and underway to address such
44 areas, systems, or processes. Such documentation must be available for in-
45 spection by the director.

46 41-6604. INVESTIGATION OF A CYBERSECURITY EVENT. (1) If the licensee
47 learns that a cybersecurity event has or may have occurred, the licensee or
48 an outside vendor or service provider designated to act on behalf of the li-
49 censee must conduct a prompt investigation.

1 (2) During the investigation, the licensee or an outside vendor or ser-
2 vice provider designated to act on behalf of the licensee must, to the extent
3 possible:

4 (a) Determine whether a cybersecurity event has occurred;

5 (b) Assess the nature and scope of the cybersecurity event;

6 (c) Identify any nonpublic information that may have been involved in
7 the cybersecurity event; and

8 (d) Perform or oversee reasonable measures to restore the security of
9 the information systems compromised in the cybersecurity event in order
10 to prevent further unauthorized acquisition, release, or use of nonpub-
11 lic information in the licensee's possession, custody, or control.

12 (3) If the licensee learns that a cybersecurity event has or may have
13 occurred that impacted the licensee's nonpublic information in a system
14 maintained by a third-party service provider, the licensee must complete the
15 steps listed in subsection (2) of this section or make reasonable efforts
16 to confirm and document that the third-party service provider has completed
17 those steps.

18 (4) The licensee must maintain records concerning all cybersecurity
19 events for a period of at least five (5) years from the date of the cybersecu-
20 rity event and must produce those records upon demand of the director.

21 41-6605. NOTICE OF A CYBERSECURITY EVENT. (1) Each licensee must no-
22 tify the director as promptly as possible but not later than five (5) busi-
23 ness days after a determination that a cybersecurity event has occurred when
24 either of the following criteria has been met:

25 (a) This state is the licensee's state of domicile, in the case of an in-
26 surer, or this state is the licensee's home state, in the case of a pro-
27 ducer, as those terms are defined in section 41-1002, Idaho Code, and
28 the cybersecurity event has a reasonable likelihood of materially harm-
29 ing:

30 (i) Any consumer residing in this state; or

31 (ii) Any material part of the normal operations of the licensee;
32 or

33 (b) The licensee reasonably believes that the nonpublic information
34 involved is of two hundred fifty (250) or more consumers residing in
35 this state and that the event is either of the following:

36 (i) A cybersecurity event impacting the licensee of which notice
37 is required to be provided to any government body, self-regulatory
38 agency, or any other supervisory body pursuant to any state or fed-
39 eral law; or

40 (ii) A cybersecurity event that has a reasonable likelihood of ma-
41 terially harming:

42 1. Any consumer residing in this state; or

43 2. Any material part of the normal operations of the li-
44 censee.

45 (2) The licensee must provide as much of the following information as
46 possible. The licensee must provide the information in electronic form, as
47 directed by the director. The licensee has a continuing obligation to update
48 and supplement initial and subsequent notifications to the director regard-

1 ing material changes to previously provided information relating to the cy-
2 bersecurity event:

- 3 (a) The date of the cybersecurity event;
- 4 (b) The description of how the information was exposed, lost, stolen,
5 or breached, including the specific roles and responsibilities of
6 third-party service providers, if any;
- 7 (c) How the cybersecurity event was discovered;
- 8 (d) Whether any lost, stolen, or breached information has been recov-
9 ered and, if so, how this was done;
- 10 (e) The identity of the source of the cybersecurity event;
- 11 (f) Whether the licensee has filed a police report or has notified any
12 regulatory, government, or law enforcement agencies and, if so, when
13 such notification was provided;
- 14 (g) The description of the specific types of information acquired with-
15 out authorization. Specific types of information means particular data
16 elements, including, for example, types of medical information, types
17 of financial information, or types of information allowing identifica-
18 tion of the consumer;
- 19 (h) The period during which the information system was compromised by
20 the cybersecurity event;
- 21 (i) The number of total consumers in this state affected by the cyber-
22 security event. The licensee must provide the best estimate in the ini-
23 tial report to the director and update this estimate with each subse-
24 quent report to the director pursuant to this section;
- 25 (j) The results of any internal review identifying a lapse in either
26 automated controls or internal procedures or confirming that all auto-
27 mated controls or internal procedures were followed;
- 28 (k) The description of efforts being undertaken to remediate the situa-
29 tion that permitted the cybersecurity event to occur;
- 30 (l) A copy of the licensee's privacy policy and a statement outlining
31 the steps the licensee will take to investigate and notify consumers af-
32 fected by the cybersecurity event; and
- 33 (m) The name of a contact person who is both familiar with the cyberse-
34 curity event and authorized to act for the licensee.

35 (3) A licensee must notify each consumer residing in this state without
36 unreasonable delay after a determination that a cybersecurity event has oc-
37 curred that is reasonably likely to result in material harm to that consumer.
38 Except as provided in subsection (6) of this section, a licensee that deter-
39 mines a cybersecurity event has occurred affecting data owned or licensed by
40 another licensee must provide a notice to the owner or licensor of the data
41 affected by the cybersecurity event in place of the notification to affected
42 consumers.

- 43 (a) The licensee must provide a copy of the notice sent to consumers to
44 the director.
- 45 (b) In determining whether a cybersecurity event is reasonably likely
46 to result in material harm to consumers residing in this state under
47 this subsection, a licensee must act with the care an ordinarily prudent
48 person in like position would exercise under similar circumstances.
- 49 (c) A licensee may delay providing notice without violating this sub-
50 section if either of the following is met:

1 (i) A delay is necessary in order for the licensee to take any mea-
2 sures necessary to determine the scope of the cybersecurity event
3 and restore the reasonable integrity of the information system.
4 However, the licensee must provide the notice required under this
5 section without unreasonable delay after the licensee completes
6 the measures necessary to determine the scope of the cybersecurity
7 event and restore the reasonable integrity of the information sys-
8 tem; or

9 (ii) A law enforcement agency determines and advises the licensee
10 that providing a notice will impede a criminal or civil inves-
11 tigation or jeopardize homeland or national security. However,
12 the licensee must provide the notice required under this sec-
13 tion without unreasonable delay after the law enforcement agency
14 determines that providing the notice will no longer impede the
15 investigation or jeopardize homeland or national security.

16 (4) In the case of a cybersecurity event impacting a licensee's nonpub-
17 lic information in a system maintained by a third-party service provider, of
18 which the licensee has become aware, the licensee must treat such event as
19 it would under subsection (1) of this section unless the third-party service
20 provider provides the notice required under subsection (1) of this section
21 to the director.

22 (a) The computation of the licensee's deadlines begins on the day after
23 the third-party service provider notifies the licensee of the cyberse-
24 curity event or the licensee otherwise has actual knowledge of the cy-
25 bersecurity event, whichever is sooner.

26 (b) Nothing in this chapter prevents or abrogates an agreement between
27 a licensee and another licensee, a third-party service provider, or any
28 other party to fulfill any of the investigation requirements imposed
29 under section 41-6604, Idaho Code, or notice requirements imposed under
30 this section.

31 (5) As to notice of cybersecurity events of reinsurers to insurers:

32 (a) In the case of a cybersecurity event involving nonpublic informa-
33 tion that is used by or in the possession, custody, or control of a li-
34 censee that is acting as an assuming insurer, including an assuming in-
35 surer domiciled in another state or jurisdiction, and that does not have
36 a direct contractual relationship with the affected consumers, both of
37 the following apply:

38 (i) The assuming insurer must notify its affected ceding insurers
39 and the insurance director of its state or jurisdiction of domi-
40 cile within five (5) business days of making the determination
41 that a cybersecurity event has occurred; and

42 (ii) The ceding insurers that have a direct contractual relation-
43 ship with affected consumers must fulfill the consumer notifica-
44 tion requirements imposed under subsection (3) of this section and
45 any other notification requirements relating to a cybersecurity
46 event imposed under this section.

47 (b) In the case of a cybersecurity event involving nonpublic informa-
48 tion that is in the possession, custody, or control of a third-party
49 service provider of a licensee that is an assuming insurer, including

1 an assuming insurer domiciled in another state or jurisdiction, both of
2 the following apply:

3 (i) The assuming insurer must notify its affected ceding insurers
4 and the insurance director of its state or jurisdiction of domi-
5 cile within five (5) business days of receiving notice from its
6 third-party service provider that a cybersecurity event has oc-
7 curred; and

8 (ii) The ceding insurers that have a direct contractual relation-
9 ship with affected consumers must fulfill the consumer notifica-
10 tion requirements imposed under subsection (3) of this section and
11 any other notification requirements relating to a cybersecurity
12 event imposed under this section.

13 (c) Any licensee acting as assuming insurer will have no other notice
14 obligations relating to a cybersecurity event or other data breach un-
15 der this section.

16 (6) In the case of a cybersecurity event involving nonpublic informa-
17 tion that is in the possession, custody, or control of a licensee that is an
18 insurer or its third-party service provider for which a consumer accessed
19 the insurer's services through an independent insurance producer, and for
20 which consumer notice is required under subsection (3) of this section, the
21 insurer must notify the producers of record of all affected consumers of the
22 cybersecurity event no later than the time at which notice is provided to
23 the affected consumers. The insurer is excused from this obligation for any
24 producer or producer's representative who is not authorized by law or con-
25 tract to sell, solicit, or negotiate on behalf of the insurer and in those
26 instances in which the insurer does not have the current producer of record
27 information for any individual consumer.

28 41-6606. DIRECTOR'S POWER TO EXAMINE AND INVESTIGATE. (1) The direc-
29 tor has the power to examine and investigate the affairs of any licensee to
30 determine whether the licensee has been or is engaged in any conduct in vio-
31 lation of this chapter. This power is in addition to the powers the director
32 has under chapter 2, title 41, Idaho Code. Any such investigation or exami-
33 nation will be conducted pursuant to chapter 2, title 41, Idaho Code.

34 (2) If the director has reason to believe that a licensee has been or
35 is engaged in conduct in this state that violates this chapter, the director
36 may take action that is necessary or appropriate to enforce the provisions of
37 this chapter.

38 41-6607. CONFIDENTIALITY AND SHARING OF DOCUMENTS, MATERIALS, AND
39 OTHER INFORMATION. (1) Any documents, materials, or other information in
40 the control or possession of the department that are furnished by a licensee
41 or an employee or agent thereof acting on behalf of a licensee pursuant to
42 section 41-6603 or 41-6605, Idaho Code, or that are obtained by the director
43 in an investigation or examination pursuant to section 41-6606, Idaho Code,
44 are confidential by law and privileged, are not subject to the Idaho public
45 records act, chapter 1, title 74, Idaho Code, are not subject to subpoena,
46 and are not subject to discovery or admissible in evidence in any private
47 civil action. However, the director is authorized to use the documents, ma-

1 materials, or other information in the furtherance of any regulatory or legal
2 action brought as a part of the director's duties.

3 (2) Neither the director nor any person who received documents, materi-
4 als, or other information while acting under the authority of the director is
5 permitted or required to testify in any private civil action concerning any
6 confidential documents, materials, or information subject to subsection (1)
7 of this section.

8 (3) In order to assist in the performance of the director's duties under
9 this chapter, the director:

10 (a) May share documents, materials, or other information, including
11 the confidential and privileged documents, materials, or information
12 subject to subsection (1) of this section, with other state, federal,
13 and international regulatory agencies, with the national associa-
14 tion of insurance commissioners, its affiliates or subsidiaries, and
15 with state, federal, and international law enforcement authorities,
16 provided that the recipient agrees in writing to maintain the confi-
17 dentiality and privileged status of the document, material, or other
18 information;

19 (b) May receive documents, materials, or information, including other-
20 wise confidential and privileged documents, materials, or information,
21 from the national association of insurance commissioners, its affili-
22 ates or subsidiaries and from regulatory and law enforcement officials
23 of other foreign or domestic jurisdictions and must maintain as confi-
24 dential or privileged any document, material, or information received
25 with notice or the understanding that it is confidential or privileged
26 under the laws of the jurisdiction that is the source of the document,
27 material, or information;

28 (c) May share documents, materials, or other information subject to
29 subsection (1) of this section with a third-party consultant or vendor,
30 provided the consultant agrees in writing to maintain the confidential-
31 ity and privileged status of the document, material, or other informa-
32 tion; and

33 (d) May enter into agreements governing sharing and use of information
34 consistent with this subsection.

35 (4) No waiver of any applicable privilege or claim of confidentiality
36 in the documents, materials, or information will occur as a result of dis-
37 closure to the director under this section or as a result of sharing as au-
38 thorized in subsection (3) of this section. This includes all protections
39 granted by subsection (1) of this section, including from disclosure pur-
40 suant to the Idaho public records act, by subpoena, and through discovery or
41 being admissible in evidence in any private civil action.

42 (5) Nothing in this chapter prohibits the director from releasing fi-
43 nal, adjudicated actions that are open to public inspection pursuant to the
44 Idaho public records act to a database or other clearinghouse service main-
45 tained by the national association of insurance commissioners or its affili-
46 ates or subsidiaries.

47 41-6608. EXCEPTIONS. (1) The following exceptions apply to this chap-
48 ter:

1 (a) A licensee meeting the following criteria is exempt from the provi-
2 sions of section 41-6603, Idaho Code:

3 (i) That has fewer than fifty (50) employees, excluding any inde-
4 pendent contractors;

5 (ii) That has less than five million dollars (\$5,000,000.00) in
6 gross annual revenue; and

7 (iii) That has less than ten million dollars (\$10,000,000.00) in
8 year-end total assets.

9 (b) A licensee that is subject to the health insurance portability and
10 accountability act of 1996 and any amendments thereto (HIPAA), that has
11 established and maintains a written information security program pur-
12 suant to statutes, rules, regulations, procedures, or guidelines es-
13 tablished under HIPAA, and that maintains nonpublic information in the
14 same manner as protected health information, will be considered to meet
15 the requirements of this chapter except for the director notification
16 requirements in section 41-6605(1), Idaho Code.

17 (c) An employee, agent, representative, or designee of a licensee,
18 who is also a licensee, is exempt from sections 41-6603, 41-6604, and
19 41-6605, Idaho Code, and need not develop its own information security
20 program to the extent that the employee, agent, representative, or
21 designee is covered by the information security program of the other
22 licensee.

23 (d) A licensee that is a financial institution or affiliated with a
24 financial institution as defined in 15 U.S.C. 6809 that maintains an
25 information security program in compliance with the interagency guide-
26 lines establishing standards for safeguarding customer information as
27 set forth pursuant to sections 501 and 505 of the Gramm-Leach-Bliley
28 act, 15 U.S.C. 6801 and 6805, will be considered to meet the require-
29 ments of section 41-6603, Idaho Code, with respect to establishing an
30 information security program, provided that the information security
31 program includes the protection of nonpublic information and the li-
32 censee's information system, and provided that the licensee produces,
33 upon request, documentation satisfactory to the director that inde-
34 pendently validates the financial institution or affiliated financial
35 institution's adoption of an information security program that satis-
36 fies the interagency guidelines.

37 (e) A licensee that is in compliance with another jurisdiction's man-
38 dated written insurance data security requirements that are at least as
39 restrictive as this chapter will be considered to meet the requirements
40 of section 41-6603, Idaho Code, with respect to establishing an infor-
41 mation security program.

42 (2) In the event that a licensee ceases to qualify for an exception,
43 such licensee has one hundred eighty (180) days to comply with this chapter.

44 41-6609. NO PRIVATE CAUSE OF ACTION. This chapter does not create or
45 imply a private cause of action for violation of its provisions or any rules
46 promulgated pursuant to it.

1 41-6610. PENALTIES FOR VIOLATION OF CHAPTER. In the case of a viola-
2 tion of this chapter, a licensee may be subject to civil penalties in accor-
3 dance with section 41-117, Idaho Code.

4 41-6611. EXCLUSIVE STATE STANDARDS AND REQUIREMENTS. Notwithstanding
5 any other provision of law, the provisions of this chapter and any rules
6 adopted pursuant to this chapter constitute the exclusive state standards
7 and requirements applicable to licensees regarding an information security
8 program, cybersecurity events, the security of nonpublic information, data
9 security, investigation of cybersecurity events, notice of cybersecurity
10 events, and notification to the director of cybersecurity events. The re-
11 quirements of sections 28-51-104, 28-51-105, 28-51-106, and 28-51-107,
12 Idaho Code, do not apply to a licensee.

13 41-6612. RULEMAKING AUTHORITY. The director may promulgate such
14 rules as are necessary to carry out the provisions of this chapter.

15 41-6613. CONSIDERATIONS IN ADMINISTERING CHAPTER. The director will
16 consider the nature, scale, and complexity of licensees in administering
17 this chapter and adopting rules pursuant to this chapter.

18 41-6614. EFFECTIVE DATE. This chapter takes effect on July 1, 2021,
19 provided that a licensee has until July 1, 2022, to comply with section
20 41-6603, Idaho Code, except for subsection (6) of that section. A licensee
21 has until July 1, 2023, to comply with section 41-6603(6), Idaho Code.

22 41-6615. SEVERABILITY. If any provision of this chapter or the appli-
23 cation thereof to any person or circumstance is for any reason held to be in-
24 valid, the remainder of the chapter and the application of such provision to
25 other persons or circumstances will not be affected thereby.