
SENATE BILL 5956

State of Washington

67th Legislature

2022 Regular Session

By Senator Stanford; by request of Insurance Commissioner

1 AN ACT Relating to insurance data security; adding a new chapter
2 to Title 48 RCW; prescribing penalties; and providing an effective
3 date.

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

5 NEW SECTION. **Sec. 1.** This chapter may be known and cited as the
6 insurance data security act.

7 NEW SECTION. **Sec. 2.** (1) The purpose and intent of this act is
8 to establish standards for data security and standards for the
9 investigation of and notification to the commissioner of a
10 cybersecurity event applicable to licensees, as defined in section 3
11 of this act.

12 (2) This act may not be construed to create or imply a private
13 cause of action for violation of its provisions nor may it be
14 construed to curtail a private cause of action which would otherwise
15 exist in the absence of this act.

16 (3) Nothing in this act may be construed or interpreted as
17 preempting, superseding, or otherwise limiting the attorney general's
18 authority to enforce either chapter 19.255 or 19.86 RCW, or both.

1 NEW SECTION. **Sec. 3.** The definitions in this section apply
2 throughout this chapter unless the context clearly requires
3 otherwise.

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

8 (2) "Commissioner" means the insurance commissioner of this
9 state.

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

15 (4) "Cybersecurity event" means an event resulting in
16 unauthorized access to, disruption, or misuse of, an information
17 system or nonpublic information stored on the information system.

18 (a) "Cybersecurity event" does not include the unauthorized
19 acquisition of encrypted nonpublic information if the encryption,
20 process, or key is not also acquired, released, or used without
21 authorization.

22 (b) "Cybersecurity event" does not include an event with regard
23 to which the licensee has determined that the nonpublic information
24 accessed by an unauthorized person has not been used or released and
25 has been returned or destroyed.

26 (5) "Encrypted" means the transformation of data into a form
27 which results in a low probability of assigning meaning without the
28 use of a protective process or key.

29 (6) "Information security program" means the administrative,
30 technical, and physical safeguards that a licensee uses to access,
31 collect, distribute, process, protect, store, use, transmit, dispose
32 of, or otherwise handle nonpublic information.

33 (7) "Information system" means a discrete set of electronic
34 information resources organized for the collection, processing,
35 maintenance, use, sharing, dissemination, or disposition of
36 electronic information, as well as any specialized system such as
37 either industrial or process, or both, control systems, telephone
38 switching and private branch exchange systems, and environmental
39 control systems.

1 (8) "Licensee" means any person licensed, authorized, or
2 registered, or required to be licensed, authorized, or registered
3 under Title 48 RCW, but does not include a purchasing group or a risk
4 retention group chartered and licensed in a state other than this
5 state or a licensee that is acting as an assuming insurer that is
6 domiciled in another state or jurisdiction.

7 (9) "Multifactor authentication" means authentication through
8 verification of at least two of the following types of authentication
9 factors:

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

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

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

14 (10) "Nonpublic information" means information that is not
15 publicly available information and is:

16 (a) Business-related information of a licensee the tampering with
17 which, or unauthorized disclosure, access, or use of which, would
18 cause a material adverse impact to the business, operations, or
19 security of the licensee;

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

24 (i) Social security number;

25 (ii) Driver's license number or nondriver identification card
26 number;

27 (iii) Account number or credit or debit card number;

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

30 (v) Biometric records; or

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

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

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

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

39 (11) "Person" has the same meaning as in RCW 48.01.070.

1 (12)(a) "Publicly available information" means any information
2 that a licensee has a reasonable basis to believe is lawfully made
3 available to the general public from: Federal, state, or local
4 government records; widely distributed media; or disclosures to the
5 general public that are required to be made by federal, state, or
6 local law.

7 (b) For the purposes of this definition, a licensee has a
8 reasonable basis to believe that information is lawfully made
9 available to the general public if the licensee has taken steps to
10 determine:

11 (i) That the information is of the type that is available to the
12 general public; and

13 (ii) Whether a consumer can direct that the information not be
14 made available to the general public and, if so, that the consumer
15 has not done so.

16 (13) "Risk assessment" means the risk assessment that each
17 licensee is required to conduct under section 4(3) of this act.

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

22 NEW SECTION. **Sec. 4.** (1) Commensurate with the size and
23 complexity of the licensee, the nature and scope of the licensee's
24 activities, including its use of third-party service providers, and
25 the sensitivity of the nonpublic information used by the licensee or
26 in the licensee's possession, custody, or control, each licensee must
27 develop, implement, and maintain a comprehensive written information
28 security program based on the licensee's risk assessment and that
29 contains administrative, technical, and physical safeguards for the
30 protection of nonpublic information and the licensee's information
31 system.

32 (2) A licensee's information security program must be designed
33 to:

34 (a) Protect the security and confidentiality of nonpublic
35 information and the security of the information system;

36 (b) Protect against any threats or hazards to the security or
37 integrity of nonpublic information and the information system;

38 (c) Protect against unauthorized access to or use of nonpublic
39 information, and minimize the likelihood of harm to any consumer; and

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

4 (3) As part of its risk assessment, the licensee must:

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

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

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

17 (d) Assess the sufficiency of policies, procedures, information
18 systems, and other safeguards in place to manage these threats,
19 including consideration of threats in each relevant area of the
20 licensee's operations, and including:

21 (i) Employee training and management;

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

25 (iii) Detecting, preventing, and responding to attacks,
26 intrusions, or other system failures; and

27 (e) Implement information safeguards to manage the threats
28 identified in its ongoing assessment, and no less than annually,
29 assess the effectiveness of the safeguards' key controls, systems,
30 and procedures.

31 (4) Based on its risk assessment, the licensee must:

32 (a) Design its information security program to mitigate the
33 identified risks, commensurate with the size and complexity of the
34 licensee, the nature and scope of the licensee's activities,
35 including its use of third-party service providers, and the
36 sensitivity of the nonpublic information used by the licensee or in
37 the licensee's possession, custody, or control;

38 (b) Determine which of the following security measures are
39 appropriate and implement the appropriate security measures
40 accordingly:

1 (i) Place access controls on information systems, including
2 controls to authenticate and permit access only to authorized
3 individuals to protect against the unauthorized acquisition of
4 nonpublic information;

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

9 (iii) Restrict physical access to nonpublic information to
10 authorized individuals only;

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

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

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

21 (vii) Utilize effective controls, which may include multifactor
22 authentication procedures for any individual accessing nonpublic
23 information;

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

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

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

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

37 (c) Include cybersecurity risks in the licensee's enterprise risk
38 management process;

39 (d) Stay informed regarding emerging threats or vulnerabilities
40 and utilize reasonable security measures when sharing information

1 relative to the character of the sharing and the type of information
2 shared; and

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

6 (5)(a) If the licensee has a board of directors, the board or an
7 appropriate committee of the board must, at a minimum:

8 (i) Require the licensee's executive management or its delegates
9 to develop, implement, and maintain the licensee's information
10 security program; and

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

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

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

21 (b) If executive management delegates any of its responsibilities
22 under this section, it must oversee the development, implementation,
23 and maintenance of the licensee's information security program
24 prepared by the delegate or delegates and must receive a report from
25 the delegate or delegates complying with the requirements of the
26 report to the board of directors under (a)(ii) of this subsection.

27 (6)(a) A licensee must exercise due diligence in selecting its
28 third-party service provider; and

29 (b) A licensee must require a third-party service provider to
30 implement appropriate administrative, technical, and physical
31 measures to protect and secure the information systems and nonpublic
32 information that are accessible to, or held by, the third-party
33 service provider.

34 (7) The licensee must monitor, evaluate, and adjust, as
35 appropriate, the information security program consistent with any
36 relevant changes in technology, the sensitivity of its nonpublic
37 information, internal or external threats to information, and the
38 licensee's own changing business arrangements, such as mergers and
39 acquisitions, alliances and joint ventures, outsourcing arrangements,
40 and changes to information systems.

1 (8) (a) As part of its information security program, each licensee
2 must establish a written incident response plan designed to promptly
3 respond to, and recover from, any cybersecurity event that
4 compromises the confidentiality, integrity, or availability of
5 nonpublic information in its possession, the licensee's information
6 systems, or the continuing functionality of any aspect of the
7 licensee's business or operations.

8 (b) The incident response plan must address the following areas:

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

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

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

13 (iv) External and internal communications and information
14 sharing;

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

17 (vi) Documentation and reporting regarding cybersecurity events
18 and related incident response activities; and

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

21 (9) Annually, each insurer domiciled in this state must submit to
22 the commissioner, a written statement by April 15th of each year,
23 certifying that the insurer is in compliance with the requirements
24 set forth in this section. Each insurer must maintain for examination
25 by the commissioner all records, schedules, and data supporting this
26 certificate for a period of five years. To the extent an insurer has
27 identified areas, systems, or processes that require material
28 improvement, updating, or redesign, the insurer must document the
29 identification and the remedial efforts planned and underway to
30 address the areas, systems, or processes. The documentation must be
31 available for inspection by the commissioner.

32 NEW SECTION. **Sec. 5.** (1) If a licensee learns that a
33 cybersecurity event has or may have occurred the licensee or either
34 an outside vendor or service provider, or both, designated to act on
35 behalf of the licensee, must conduct a prompt investigation.

36 (2) During the investigation, the licensee, or either an outside
37 vendor or service provider, or both, designated to act on behalf of
38 the licensee, must, at a minimum determine as much of the following
39 information as possible:

- 1 (a) Determine whether a cybersecurity event has occurred;
- 2 (b) Assess the nature and scope of the cybersecurity event;
- 3 (c) Identify any nonpublic information that may have been
- 4 involved in the cybersecurity event; and
- 5 (d) Perform or oversee reasonable measures to restore the
- 6 security of the information systems compromised in the cybersecurity
- 7 event in order to prevent further unauthorized acquisition, release,
- 8 or use of nonpublic information in the licensee's possession,
- 9 custody, or control.

10 (3) If the licensee learns that a cybersecurity event has or may
11 have occurred in a system maintained by a third-party service
12 provider, the licensee must complete the steps listed in subsection
13 (2) of this section or confirm and document that the third-party
14 service provider has completed those steps.

15 (4) The licensee must maintain records concerning all
16 cybersecurity events for a period of at least five years from the
17 date of the cybersecurity event and must produce those records upon
18 demand of the commissioner.

19 NEW SECTION.

Sec. 6.

(1) Each licensee must notify the
20 commissioner as promptly as possible but in no event later than three
21 business days from a determination that a cybersecurity event has
22 occurred when either of the following criteria has been met:

23 (a)(i) This state is the licensee's state of domicile, in the
24 case of an insurer, as that term is defined in RCW 48.17.010;

25 (ii) This state is the licensee's home state, in the case of an
26 insurance producer, as that term is defined in RCW 48.17.010; or

27 (iii) When the licensee is not an insurer or an insurance
28 producer, the licensee is a person who is either formed under the
29 laws of this state, or whose residence or principal place of business
30 is located in this state, or both; or

31 (b) The licensee reasonably believes that the nonpublic
32 information involved is of 250 or more consumers residing in this
33 state and that is either of the following:

34 (i) A cybersecurity event impacting the licensee of which notice
35 is required to be provided to any government body, self-regulatory
36 agency, or any other supervisory body under any state or federal law;
37 or

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

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

2 (B) Any material part of the normal operation or operations of
3 the licensee.

4 (2)(a) As part of the notification to the commissioner required
5 under subsection (1) of this section, the licensee must provide as
6 much of the following information as possible:

7 (i) Date of the cybersecurity event;

8 (ii) Description of how the information was exposed, lost,
9 stolen, or breached, including the specific roles and
10 responsibilities of third-party service providers, if any;

11 (iii) How the cybersecurity event was discovered;

12 (iv) Whether any lost, stolen, or breached information has been
13 recovered and if so, how this was done;

14 (v) The identity of the source of the cybersecurity event;

15 (vi) Whether the licensee has filed a police report or has
16 notified any regulatory, government, or law enforcement agencies and,
17 if so, when such notification was provided;

18 (vii) Description of the specific types of information accessed
19 or acquired without authorization. Specific types of information
20 means particular data elements including, for example, types of
21 medical information, types of financial information, or types of
22 information allowing identification of the consumer;

23 (viii) The period during which the information system was
24 compromised by the cybersecurity event;

25 (ix) The number of total consumers in this state affected by the
26 cybersecurity event. The licensee must provide the best estimate in
27 the initial report to the commissioner and update this estimate with
28 each subsequent report to the commissioner under this section;

29 (x) The results of any internal review identifying a lapse in
30 either automated controls or internal procedures, or confirming that
31 all automated controls or internal procedures were followed;

32 (xi) Description of efforts being undertaken to remediate the
33 situation that permitted the cybersecurity event to occur;

34 (xii) A copy of the licensee's privacy policy and a statement
35 outlining the steps the licensee will take to investigate and notify
36 consumers affected by the cybersecurity event; and

37 (xiii) Name of a contact person who is both familiar with the
38 cybersecurity event and authorized to act for the licensee.

39 (b) The licensee must provide the information in electronic form
40 as directed by the commissioner. The licensee has a continuing

1 obligation to update and supplement initial and subsequent
2 notifications to the commissioner concerning the cybersecurity event,
3 as new information dictates.

4 (3) Licensees must comply with chapter 19.255 RCW, as applicable,
5 and provide notice to the attorney general and a copy of the notice
6 sent to consumers under that chapter to the commissioner, when a
7 licensee is required to notify the commissioner under subsection (1)
8 of this section.

9 (4)(a) In the case of a cybersecurity event in a system
10 maintained by a third-party service provider, of which the licensee
11 has become aware, the licensee must treat the event as it would under
12 subsection (1) of this section.

13 (b) The computation of licensee's deadlines begins on the day
14 after the third-party service provider notifies the licensee of the
15 cybersecurity event or the licensee otherwise has actual knowledge of
16 the cybersecurity event, whichever is sooner.

17 (c) Nothing in this chapter prevents or abrogates an agreement
18 between a licensee and another licensee, a third-party service
19 provider, or any other party to fulfill any of the investigation
20 requirements imposed under section 5 of this act or notice
21 requirements imposed under this section.

22 (5)(a)(i) In the case of a cybersecurity event involving
23 nonpublic information that is used by the licensee that is acting as
24 an assuming insurer or in the possession, custody, or control of a
25 licensee that is acting as an assuming insurer and that does not have
26 a direct contractual relationship with the affected consumers, the
27 assuming insurer must notify its affected ceding insurers and the
28 commissioner of its state of domicile within three business days of
29 making the determination that a cybersecurity event has occurred.

30 (ii) The ceding insurers that have a direct contractual
31 relationship with affected consumers must fulfill the consumer
32 notification requirements imposed under chapter 19.255 RCW and any
33 other notification requirements relating to a cybersecurity event
34 imposed under this section.

35 (b)(i) In the case of a cybersecurity event involving nonpublic
36 information that is in the possession, custody, or control of a
37 third-party service provider of a licensee that is an assuming
38 insurer, the assuming insurer must notify its affected ceding
39 insurers and the commissioner of its state of domicile within three

1 business days of receiving notice from its third-party service
2 provider that a cybersecurity event has occurred.

3 (ii) The ceding insurers that have a direct contractual
4 relationship with affected consumers must fulfill the consumer
5 notification requirements imposed under chapter 19.255 RCW and any
6 other notification requirements relating to a cybersecurity event
7 imposed under this section.

8 (6) (a) In the case of a cybersecurity event involving nonpublic
9 information that is in the possession, custody, or control of a
10 licensee that is an insurer or its third-party service provider and
11 for which a consumer accessed the insurer's services through an
12 independent insurance producer, the insurer must notify the producers
13 of record of all affected consumers no later than the insurer gives
14 notice to consumers as required under RCW 19.255.010.

15 (b) The insurer is excused from this obligation for those
16 instances in which it does not have the current insurance producer of
17 record information for any individual consumer.

18 NEW SECTION. **Sec. 7.** (1) The commissioner has power to examine
19 and investigate into the affairs of any licensee to determine whether
20 the licensee has been or is engaged in any conduct in violation of
21 this act. This power is in addition to the powers which the
22 commissioner has under this title. Any investigation or examination
23 must be conducted under this title.

24 (2) Whenever the commissioner has reason to believe that a
25 licensee has been or is engaged in conduct in this state which
26 violates this act, the commissioner may take action that is necessary
27 or appropriate to enforce the provisions of this act.

28 NEW SECTION. **Sec. 8.** (1) Any documents, materials, or other
29 information in the control or possession of the commissioner that are
30 furnished by a licensee or an employee or agent acting on behalf of a
31 licensee under sections 4(9) and 6(2)(a) (ii) through (v), (viii),
32 (x), and (xi) of this act, or that are obtained by the commissioner
33 in an investigation or examination under section 7 of this act are
34 confidential, are not subject to chapter 42.56 RCW, are not subject
35 to subpoena, and are not subject to discovery or admissible in
36 evidence in any private civil action. However, the commissioner is
37 authorized to use the documents, materials, or other information in

1 the furtherance of any regulatory or legal action brought as a part
2 of the commissioner's regular duties.

3 (2) Neither the commissioner nor any person who received
4 documents, materials, or other information while acting under the
5 authority of the commissioner, or with whom the documents, materials,
6 or other information are shared under this chapter are required to
7 testify in any private civil action concerning any confidential
8 documents, materials, or information subject to subsection (1) of
9 this section.

10 (3) In order to assist in the performance of the commissioner's
11 duties under this act, the commissioner may:

12 (a) Share documents, materials, or other information, including
13 the confidential and privileged documents, materials, or information
14 subject to subsection (1) of this section, with the following
15 recipients provided that the recipient agrees in writing to maintain
16 the confidentiality and privileged status of the documents,
17 materials, or other information: The attorney general; other state,
18 federal, and international regulatory agencies; the national
19 association of insurance commissioners and its affiliates or
20 subsidiaries; and state, federal, and international law enforcement
21 authorities. The attorney general is bound by separate
22 confidentiality and trade secret authorities;

23 (b) Receive documents, materials, or information, including
24 otherwise confidential and privileged documents, materials, or
25 information, from the national association of insurance commissioners
26 and its affiliates or subsidiaries, and from regulatory and law
27 enforcement officials of other foreign or domestic jurisdictions. The
28 commissioner shall maintain as confidential or privileged any
29 documents, materials, or information received with notice or
30 understanding that they are confidential or privileged under the laws
31 of the jurisdiction that is the source of the documents, materials,
32 or information;

33 (c) Share documents, materials, or other information subject to
34 subsection (1) of this section, with a third-party consultant or
35 vendor provided the consultant agrees in writing to maintain the
36 confidentiality and privileged status of the documents, materials, or
37 other information; and

38 (d) Enter into agreements governing sharing and use of
39 information consistent with this subsection.

1 (4) A waiver of any applicable privilege or claim of
2 confidentiality in the documents, materials, or information does not
3 occur as a result of disclosure to the commissioner under this
4 section or as a result of sharing as authorized in subsection (3) of
5 this section.

6 (5) Nothing in this chapter prohibits the commissioner from
7 releasing final, adjudicated actions that are open to public
8 inspection under chapter 42.56 RCW to a database or other
9 clearinghouse service maintained by the national association of
10 insurance commissioners and its affiliates or subsidiaries.

11 (6) Any documents, materials, or other information in the control
12 or possession of the national association of insurance commissioners
13 or a third-party consultant or vendor under sections 4(9) and 6(2)(a)
14 (ii) through (v), (viii), (x), and (xi) of this act, or that are
15 obtained by the commissioner in an investigation or examination under
16 section 7 of this act are confidential, are not subject to chapter
17 42.56 RCW, are not subject to subpoena, and are not subject to
18 discovery or admissible in evidence in any private civil action.

19 (7)(a) If the licensee contacts a law enforcement agency after
20 learning of a cybersecurity event that has or may have occurred and
21 the law enforcement agency determines that the notification required
22 under chapter 19.255 RCW will impede a criminal investigation, the
23 licensee must still provide the notice to the commissioner as
24 required by section 6 of this act.

25 (b) Until the law enforcement agency determines that the
26 disclosure required under chapter 19.255 RCW will not compromise the
27 investigation, any documents, materials, or other information in the
28 control or possession of the commissioner that are furnished by a
29 licensee, or an employee or agent acting on behalf of a licensee
30 under section 6 of this act, are confidential, are not subject to
31 chapter 42.56 RCW, are not subject to subpoena, and are not subject
32 to discovery or admissible in evidence in any private civil action.
33 However, the commissioner is permitted to share the documents,
34 materials, and other information as provided in subsection (3) of
35 this section.

36 (c) After the law enforcement agency has determined that the
37 disclosure required under chapter 19.255 RCW will not compromise the
38 investigation, the confidentiality provided under subsections (1) and
39 (6) of this section apply.

1 NEW SECTION. **Sec. 9.** (1) The following exceptions apply to this
2 chapter:

3 (a) A licensee with fewer than 10 employees, including any
4 independent contractors, is exempt from section 4 of this act;

5 (b) A licensee subject to the federal health insurance
6 portability and accountability act (P.L. 104-191, August 21, 1996,
7 110 Stat. 1936) that has established and maintains an information
8 security program under the statutes, rules, regulations, procedures,
9 or guidelines established under that act, will be considered to meet
10 the requirements of section 4 of this act, provided that the licensee
11 is compliant with, and submits a written statement certifying its
12 compliance with, section 4 of this act;

13 (c) An employee, agent, representative, or designee of a
14 licensee, who is also a licensee, is exempt from section 4 of this
15 act and need not develop its own information security program to the
16 extent that the employee, agent, representative, or designee is
17 covered by the information security program of the other licensee.

18 (2) In the event that a licensee ceases to qualify for an
19 exception, the licensee has 180 days to comply with this chapter.

20 NEW SECTION. **Sec. 10.** In the case of a violation of this
21 chapter, a licensee may be penalized under any penalty provision of
22 this code applicable to that licensee.

23 NEW SECTION. **Sec. 11.** The commissioner may adopt rules to
24 implement and administer this chapter.

25 NEW SECTION. **Sec. 12.** If any provision of this act or its
26 application to any person or circumstance is held invalid, the
27 remainder of the act or the application of the provision to other
28 persons or circumstances is not affected.

29 NEW SECTION. **Sec. 13.** (1) This act takes effect July 1, 2022.

30 (2) Except for section 4(6) of this act, licensees have one year
31 from the effective date of this section to implement section 4 of
32 this act. Licensees have two years from the effective date of this
33 section to implement section 4(6) of this act.

1 NEW SECTION. **Sec. 14.** Sections 1 through 11 of this act
2 constitute a new chapter in Title 48 RCW.

--- **END** ---