

SENATE/HOUSE FILE _____
BY (PROPOSED DEPARTMENT OF
COMMERCE/INSURANCE DIVISION
BILL)

A BILL FOR

1 An Act relating to standards for data security, and
2 investigations and notifications of cybersecurity events,
3 for certain licensees under the jurisdiction of the
4 commissioner of insurance, making penalties applicable, and
5 including effective date provisions.
6 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

1 Section 1. NEW SECTION. 507F.1 Title.

2 This chapter may be cited as the "*Insurance Data Security*
3 *Act*".

4 Sec. 2. NEW SECTION. 507F.2 Purpose and scope.

5 1. Notwithstanding any provision of law to the contrary,
6 this chapter establishes the exclusive state standards for
7 data security, and the investigation and notification of
8 cybersecurity events, applicable to licensees.

9 2. This chapter shall not be construed to create or imply
10 a private cause of action for a violation of its provisions,
11 and shall not be construed to curtail a private cause of action
12 that otherwise exists in the absence of this chapter.

13 Sec. 3. NEW SECTION. 507F.3 Definitions.

14 As used in this chapter, unless the context otherwise
15 requires:

16 1. "*Authorized individual*" means an individual known to
17 and screened by a licensee and determined to be necessary and
18 appropriate to have access to nonpublic information held by the
19 licensee and the licensee's information system.

20 2. "*Commissioner*" means the commissioner of insurance.

21 3. "*Consumer*" means an individual, including but not limited
22 to an applicant, policyholder, insured, beneficiary, claimant,
23 or certificate holder, who is a resident of this state and
24 whose nonpublic information is in a licensee's possession,
25 custody, or control.

26 4. "*Cybersecurity event*" means an event resulting in
27 unauthorized access to, or the disruption or misuse of, an
28 information system or of nonpublic information stored on an
29 information system. "*Cybersecurity event*" does not include any
30 of the following:

31 a. The unauthorized acquisition of encrypted nonpublic
32 information if the encryption, process, or key is not also
33 acquired, released, or used without authorization.

34 b. An event for which a licensee has determined that the
35 nonpublic information accessed by an unauthorized person has

1 not been used or released, and the nonpublic information has
2 been returned or destroyed.

3 5. *"Delivered by electronic means"* means delivery to an
4 electronic mail address at which a consumer has consented to
5 receive notices or documents.

6 6. *"Encrypted"* means the transformation of data into a form
7 that results in a low probability of assigning meaning to the
8 data without the use of a protective process or key.

9 7. *"Health Insurance Portability and Accountability
10 Act"* or *"HIPAA"* means the Health Insurance Portability and
11 Accountability Act of 1996, Pub. L. No. 104-191, including
12 amendments thereto and regulations promulgated thereunder.

13 8. *"Home state"* means the same as defined in section 522B.1.

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

19 10. *"Information system"* means a discrete set of electronic
20 information resources organized for the collection, processing,
21 maintenance, use, sharing, dissemination, or disposition of
22 electronic information, and any specialized system such as an
23 industrial or process controls system, a telephone switching
24 and private branch exchange system, or an environmental control
25 system.

26 11. *"Insurer"* means the same as defined in section 521A.1.

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

34 13. *"Multi-factor authentication"* means authentication
35 through verification of at least two of the following types of

1 authentication factors:

2 *a.* A knowledge factor, such as a password.

3 *b.* A possession factor, such as a token or text message on a
4 mobile phone.

5 *c.* An inherence factor, such as a biometric characteristic.

6 14. "*Nonpublic information*" means electronic information
7 that is not publicly available information and that is any of
8 the following:

9 *a.* Business-related information of a licensee the tampering
10 of which, or unauthorized disclosure, access, or use of
11 which, will cause a material adverse impact to the business,
12 operations, or security of the licensee.

13 *b.* Information concerning a consumer which can be used to
14 identify the consumer due to a name, number, personal mark, or
15 other identifier, used in combination with any one or more of
16 the following data elements:

17 (1) A social security number.

18 (2) A driver's license number or a nondriver identification
19 card number.

20 (3) A financial account number, a credit card number, or a
21 debit card number.

22 (4) A security code, an access code, or a password that will
23 permit access to a consumer's financial accounts.

24 (5) A biometric record.

25 *c.* Information or data, except age or gender, in any form or
26 medium created by or derived from a health care provider or a
27 consumer, and that relates to any of the following:

28 (1) The past, present, or future physical, mental or
29 behavioral health or condition of a consumer, or a member of
30 the consumer's family.

31 (2) The provision of health care services to a consumer.

32 (3) Payment for the provision of health care services to a
33 consumer.

34 15. "*Person*" means an individual or a nongovernmental
35 entity, including but not limited to a nongovernmental

1 partnership, corporation, branch, agency, or association.

2 16. "*Publicly available information*" means information
3 that a licensee has a reasonable basis to believe is lawfully
4 made available to the general public from federal, state, or
5 local government records, by widely distributed media, or by
6 disclosure to the general public as required by federal, state,
7 or local law. For purposes of this definition, a licensee has
8 a reasonable basis to believe that information is lawfully made
9 available to the general public if the licensee has determined
10 all of the following:

11 a. That the information is of a type that is available to
12 the general public.

13 b. That if a consumer may direct that the information not
14 be made available to the general public, that the consumer has
15 not directed that the information not be made available to the
16 general public.

17 17. "*Risk assessment*" means the assessment that a licensee
18 is required to conduct pursuant to section 507F.4, subsection
19 3.

20 18. "*Third-party service provider*" means a person that is
21 not a licensee that contracts with a licensee to maintain,
22 process, store, or is otherwise permitted access to nonpublic
23 information through the person's provision of services to the
24 licensee.

25 Sec. 4. NEW SECTION. 507F.4 **Information security program.**

26 1. a. Commensurate with the size and complexity of a
27 licensee, the nature and scope of a licensee's activities
28 including the licensee's use of third-party service providers,
29 and the sensitivity of nonpublic information used by the
30 licensee or that is in the licensee's possession, custody, or
31 control, the licensee shall develop, implement, and maintain a
32 comprehensive written information security program based on the
33 licensee's risk assessment conducted pursuant to subsection 3.

34 b. This section shall not apply to any of the following:

35 (1) A licensee that meets any of the following criteria:

1 (a) Has fewer than ten individuals on its workforce,
2 including employees and independent contractors.

3 (b) Has less than five million dollars in gross annual
4 revenue.

5 (c) Has less than ten million dollars in year-end total
6 assets.

7 (2) An employee, agent, representative, or designee of a
8 licensee, and the employee, agent, representative, or designee
9 is also a licensee, if the employee, agent, representative, or
10 designee is covered by the information security program of the
11 other licensee.

12 c. A licensee shall have one hundred eighty calendar days
13 from the date the licensee no longer qualifies for exemption
14 under paragraph "b" to comply with this section.

15 2. A licensee's information security program must be
16 designed to do all of the following:

17 a. Protect the security and confidentiality of nonpublic
18 information and the security of the licensee's information
19 system.

20 b. Protect against threats or hazards to the security
21 or integrity of nonpublic information and the licensee's
22 information system.

23 c. Protect against unauthorized access to or the use of
24 nonpublic information, and minimize the likelihood of harm to
25 any consumer.

26 d. Define and periodically reevaluate a schedule for
27 retention of nonpublic information and a mechanism for the
28 destruction of nonpublic information if retention is no longer
29 necessary for the licensee's business operations, or is no
30 longer required by applicable law.

31 3. A licensee shall conduct a risk assessment that
32 accomplishes all of the following:

33 a. Designates one or more employees, an affiliate, or an
34 outside vendor to act on behalf of the licensee and that has
35 responsibility for the information security program.

1 *b.* Identifies reasonably foreseeable internal or external
2 threats that may result in unauthorized access, transmission,
3 disclosure, misuse, alteration, or destruction of nonpublic
4 information, including nonpublic information that is accessible
5 to, or held by, a third-party service provider.

6 *c.* Assesses the probability of, and the potential damage
7 caused by, the threats identified in paragraph "*b*", taking into
8 consideration the sensitivity of nonpublic information.

9 *d.* Assesses the sufficiency of policies, procedures,
10 information systems, and other safeguards in place to manage
11 the threats identified in paragraph "*b*". This assessment must
12 include consideration of threats identified in each relevant
13 area of the licensee's operations, including all of the
14 following:

15 (1) Employee training and management.

16 (2) Information systems, including network and software
17 design; and information classification, governance, processing,
18 storage, transmission, and disposal.

19 (3) Detection, prevention, and response to an attack,
20 intrusion, or other system failure.

21 *e.* Implements information safeguards to manage threats
22 identified in the licensee's ongoing risk assessments and, at
23 least annually, assesses the effectiveness of the information
24 safeguards' key controls, systems, and procedures.

25 4. Based on the risk assessment conducted pursuant to
26 subsection 3, a licensee shall do all of the following:

27 *a.* Develop, implement, and maintain an information security
28 program as described in subsections 1 and 2.

29 *b.* Determine which of the following security measures are
30 appropriate and implement each appropriate security measure:

31 (1) Place access controls on information systems, including
32 controls to authenticate and permit access only to authorized
33 individuals to protect against the unauthorized acquisition of
34 nonpublic information.

35 (2) Identify and manage the data, personnel, devices,

1 systems, and facilities that enable the licensee to achieve
2 its business purposes in accordance with the data, personnel,
3 devices, systems, and facilities relative importance to the
4 licensee's business objectives and risk strategy.

5 (3) Restrict access of nonpublic information stored in or at
6 physical locations to authorized individuals only.

7 (4) Protect by encryption or other appropriate means,
8 all nonpublic information while the nonpublic information
9 is transmitted over an external network, and all nonpublic
10 information that is stored on a laptop computer, a portable
11 computing or storage device, or portable computing or storage
12 media.

13 (5) Adopt secure development practices for in-house
14 developed applications utilized by the licensee, and procedures
15 for evaluating, assessing, and testing the security of
16 externally developed applications utilized by the licensee.

17 (6) Modify information systems in accordance with the
18 licensee's information security program.

19 (7) Utilize effective controls, which may include
20 multi-factor authentication procedures for authorized
21 individuals accessing nonpublic information.

22 (8) Regularly test and monitor systems and procedures to
23 detect actual and attempted attacks on, or intrusions into,
24 information systems.

25 (9) Include audit trails within the information security
26 program designed to detect and respond to cybersecurity events,
27 and designed to reconstruct material financial transactions
28 sufficient to support the normal business operations and
29 obligations of the licensee.

30 (10) Implement measures to protect against the destruction,
31 loss, or damage of nonpublic information due to environmental
32 hazards, natural disasters, catastrophes, or technological
33 failures.

34 (11) Develop, implement, and maintain procedures for the
35 secure disposal of nonpublic information that is contained in

1 any format.

2 *c.* Include cybersecurity risks in the licensee's
3 enterprise-wide risk management process.

4 *d.* Maintain knowledge and understanding of emerging threats
5 or vulnerabilities and utilize reasonable security measures,
6 relative to the character of the sharing and the type of
7 information being shared, when sharing information.

8 *e.* Provide the licensee's personnel with cybersecurity
9 awareness training that is updated as necessary to reflect
10 risks identified by the licensee's risk assessment.

11 5. *a.* If a licensee has a board of directors, the board
12 or an appropriate committee of the board shall at a minimum
13 require the licensee's executive management or the executive
14 management's delegates to:

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

17 (2) Provide a written report to the board, at least
18 annually, that documents all of the following:

19 (a) The overall status of the licensee's information
20 security program and the licensee's compliance with this
21 chapter.

22 (b) Material matters related to the licensee's information
23 security program including issues such as risk assessment; risk
24 management and control decisions; third-party service provider
25 arrangements; results of testing, cybersecurity events, or
26 violations; management's response to cybersecurity events or
27 violations; and recommendations for changes in the licensee's
28 information security program.

29 *b.* If a licensee's executive management delegates any of its
30 responsibilities under this section the executive management
31 shall oversee the delegate's development, implementation, and
32 maintenance of the licensee's information security program, and
33 shall require the delegate to submit an annual written report
34 to executive management that contains the information required
35 under paragraph "a", subparagraph (2). If the licensee has a

1 board of directors, the executive management shall provide a
2 copy of the report to the board.

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

12 7. As part of a licensee's information security program,
13 a licensee shall establish a written incident response
14 plan designed to promptly respond to, and recover from, a
15 cybersecurity event that compromises the confidentiality,
16 integrity, or availability of nonpublic information in the
17 licensee's possession, the licensee's information systems, or
18 the continuing functionality of any aspect of the licensee's
19 operations. The written incident response plan must address
20 all of the following:

21 a. The licensee's internal process for responding to a
22 cybersecurity event.

23 b. The goals of the licensee's incident response plan.

24 c. The assignment of clear roles, responsibilities,
25 and levels of decision-making authority for the licensee's
26 personnel that participate in the incident response plan.

27 d. External communications, internal communications, and
28 information sharing related to a cybersecurity event.

29 e. The identification of remediation requirements for
30 weaknesses identified in information systems and associated
31 controls.

32 f. Documentation and reporting regarding cybersecurity
33 events and related incident response activities.

34 g. The evaluation and revision of the incident response
35 plan, as appropriate, following a cybersecurity event.

1 8. An insurer domiciled in this state shall annually
2 submit to the commissioner on or before April 15 a written
3 certification that the insurer is in compliance with this
4 section. Each insurer shall maintain all records, schedules,
5 documentation, and data supporting the insurer's certification
6 for five years. To the extent an insurer has identified an
7 area, system, or process that requires material improvement,
8 updating, or redesign, the insurer shall document the process
9 used to identify the area, system, or process, and the
10 remediation that has been implemented, or will be implemented,
11 to address the area, system, or process. All records,
12 schedules, documentation, and data described in this subsection
13 shall be made available for inspection by the commissioner,
14 or the commissioner's representative, upon request of the
15 commissioner.

16 9. Licensees shall comply with this section no later than
17 January 1, 2023.

18 Sec. 5. NEW SECTION. 507F.5 **Third-party service provider**
19 **arrangements.**

20 1. A licensee shall exercise due diligence in the selection
21 of third-party service providers, conduct oversight of
22 all third-party service provider arrangements, and require
23 all third-party service providers to implement appropriate
24 administrative, technical, and physical measures to protect
25 and secure the information systems and nonpublic information
26 that are accessible to, or held by, the licensee's third-party
27 service providers.

28 2. Licensees shall comply with this section no later than
29 January 1, 2024.

30 Sec. 6. NEW SECTION. 507F.6 **Cybersecurity event —**
31 **investigation.**

32 1. If a licensee discovers that a cybersecurity event has
33 occurred, or that a cybersecurity event may have occurred, the
34 licensee, or the outside vendor or third-party service provider
35 the licensee has designated to act on behalf of the licensee,

1 shall conduct a prompt investigation of the event.

2 2. During the investigation, the licensee, outside vendor,
3 or third-party service provider the licensee has designated to
4 act on behalf of the licensee, shall, at a minimum, determine
5 as much of the following as possible:

6 a. Confirm that a cybersecurity event has occurred.

7 b. Assess the nature and scope of the cybersecurity event.

8 c. Identify all nonpublic information that may have been
9 compromised by the cybersecurity event.

10 d. Perform or oversee reasonable measures to restore the
11 security of any compromised information systems in order to
12 prevent further unauthorized acquisition, release, or use of
13 nonpublic information that is in the licensee's possession,
14 custody, or control.

15 3. If a licensee learns that a cybersecurity event has
16 occurred, or may have occurred, in an information system
17 maintained by a third-party service provider of the licensee,
18 the licensee shall complete an investigation in compliance with
19 this section, or confirm and document that the third-party
20 service provider has completed an investigation in compliance
21 with this section.

22 4. A licensee shall maintain all records and documentation
23 related to the licensee's investigation of a cybersecurity
24 event for a minimum of five years from the date of the event,
25 and shall produce the records and documentation upon demand of
26 the commissioner.

27 **Sec. 7. NEW SECTION. 507F.7 Cybersecurity event —**
28 **notification and report to the commissioner.**

29 1. A licensee shall notify the commissioner no later
30 than three business days from the date of the licensee's
31 confirmation of a cybersecurity event if any of the following
32 conditions apply:

33 a. The licensee is an insurer who is domiciled in this
34 state, or is a producer whose home state is this state, and any
35 of the following apply:

1 (1) State or federal law requires that notice of the
2 cybersecurity event be given by the licensee to a government
3 body, self-regulatory agency, or other supervisory body.

4 (2) The cybersecurity event has a reasonable likelihood
5 of causing material harm to a material part of the normal
6 business, operations, or security of the licensee.

7 *b.* The licensee reasonably believes that nonpublic
8 information compromised by the cybersecurity event involves two
9 hundred fifty or more consumers and either of the following
10 apply:

11 (1) State or federal law requires that notice of the
12 cybersecurity event be given by the licensee to a government
13 body, self-regulatory agency, or other supervisory body.

14 (2) The cybersecurity event has a reasonable likelihood of
15 causing material harm to a consumer, or to a material part of
16 the normal business, operations, or security of the licensee.

17 2. A licensee's notification to the commissioner pursuant
18 to subsection 1 shall provide, in the form and manner
19 prescribed by the commissioner by rule, as much of the
20 following information as is available to the licensee at the
21 time of the notification:

22 *a.* The date and time of the cybersecurity event.

23 *b.* A description of how nonpublic information was exposed,
24 lost, stolen, or breached, including the specific roles
25 and responsibilities of the licensee's third-party service
26 providers, if any.

27 *c.* How the licensee discovered or became aware of the
28 cybersecurity event.

29 *d.* If any lost, stolen, or breached nonpublic information
30 has been recovered and if so, how the recovery occurred.

31 *e.* The identity of the source of the cybersecurity event.

32 *f.* The identity of any regulatory, governmental, or law
33 enforcement agencies the licensee has notified, and the date
34 and time of each notification.

35 *g.* A description of the specific types of nonpublic

1 information that were lost, stolen, or breached.

2 *h.* The total number of consumers affected by the
3 cybersecurity event. The licensee shall provide the best
4 estimate of affected consumers in the licensee's initial report
5 to the commissioner and shall update the estimate in each
6 subsequent report to the commissioner under subsection 3.

7 *i.* The results of any internal review conducted by the
8 licensee that identified a lapse in the licensee's automated
9 controls or internal procedures, or that confirmed the
10 licensee's compliance with all automated controls or internal
11 procedures.

12 *j.* A description of the licensee's efforts to remediate the
13 circumstances that allowed the cybersecurity event.

14 *k.* A copy of the licensee's privacy policy.

15 *l.* A statement outlining the steps the licensee is taking
16 to identify and notify consumers affected by the cybersecurity
17 event.

18 *m.* The contact information for the individual authorized
19 to act on behalf of the licensee and who is also knowledgeable
20 regarding the cybersecurity event.

21 3. A licensee shall have a continuing obligation to update
22 and supplement the licensee's initial notification to the
23 commissioner as material changes to information previously
24 provided to the commissioner occur.

25 **Sec. 8. NEW SECTION. 507F.8 Cybersecurity event —**
26 **notification to consumers.**

27 1. In the event of a cybersecurity event involving nonpublic
28 information, consumer notification shall be made by the
29 licensee in the most expeditious manner possible and without
30 unreasonable delay consistent with the legitimate needs of law
31 enforcement as provided in subsection 2, and consistent with
32 any measures necessary for the licensee to identify contact
33 information for the affected consumers, determine the scope
34 of the cybersecurity event, and to restore the integrity,
35 security, and confidentiality of the licensee's information

1 system.

2 2. The consumer notification requirements under this
3 section may be delayed if a law enforcement agency determines
4 that consumer notification may impede a criminal investigation
5 and the agency has made a written request to the licensee to
6 delay the notification. The consumer notification required by
7 this section shall be made after the law enforcement agency
8 determines that the notification will not compromise the
9 investigation and provides written notice to the licensee that
10 consumer notification can proceed.

11 3. *a.* For purposes of this section, notification to an
12 affected consumer shall be provided by one of the following
13 methods:

14 (1) Written notice to the consumer's last known address that
15 the licensee has in the licensee's records.

16 (2) If the licensee's customary method of communication
17 with an affected consumer is by electronic means, or is
18 consistent with the applicable provisions regarding electronic
19 records and signatures set forth in chapter 554D and the
20 federal Electronic Signatures in Global and National Commerce
21 Act, 15 U.S.C. §7001, the notice may be delivered by electronic
22 means.

23 *b.* If a licensee demonstrates to the satisfaction of the
24 commissioner that the cost of providing notice to affected
25 consumers will exceed two hundred fifty thousand dollars, or
26 that the class of affected consumers exceeds three hundred
27 fifty thousand persons, or that the licensee does not have
28 sufficient contact information for an affected consumer to
29 provide notice, substitute notice may be used and must consist
30 of the following:

31 (1) Notice shall be delivered by electronic means if
32 the licensee has an electronic mail address for an affected
33 consumer in the licensee's records.

34 (2) Conspicuous posting of the notice, or a link to the
35 notice, on the internet site of the licensee if the licensee

1 maintains an internet site.

2 (3) Notification via major statewide media and local media
3 in all counties in which an affected consumer resides.

4 c. If a licensee is required to provide notice of a
5 cybersecurity event to the commissioner pursuant to section
6 507F.7, subsection 1, the licensee shall submit to the
7 commissioner a copy of all consumer notices provided by the
8 licensee to affected consumers under this section.

9 4. Consumer notice pursuant to this section shall include,
10 at a minimum, all of the following:

11 a. A description of the cybersecurity event.

12 b. The approximate date and time of the cybersecurity event.

13 c. The type of nonpublic information involved in the
14 cybersecurity event.

15 d. The current telephone number, internet site, and mailing
16 address of the three largest nationwide consumer reporting
17 agencies.

18 e. Advice to the consumer to report suspected incidents of
19 identity theft related to the cybersecurity event to local law
20 enforcement or the attorney general.

21 5. Notwithstanding subsection 1, notification is not
22 required if after an investigation pursuant to section 507F.6,
23 or after consultation with appropriate federal, state, or local
24 law enforcement agencies, a licensee determines that there is
25 no reasonable likelihood of financial harm to consumers whose
26 nonpublic information is affected by a cybersecurity event.
27 Such determination must be documented by the licensee in
28 writing, maintained for a minimum of five years from the date
29 of the determination, and made available to the commissioner
30 for inspection upon request of the commissioner.

31 6. A licensee that was subject to a cybersecurity event
32 requiring notification to more than five hundred consumers
33 pursuant to this section shall give written notice of the event
34 to the director of the consumer protection division of the
35 office of the attorney general within five business days of

1 the date the first notice is provided to an affected consumer
2 pursuant to this section.

3 Sec. 9. NEW SECTION. 507F.9 Cybersecurity event —
4 third-party service providers.

5 1. If a licensee becomes aware of a cybersecurity
6 event in an information system maintained by a third-party
7 service provider of the licensee, the licensee shall comply
8 with section 507F.7, or the licensee may obtain a written
9 certification from the third-party service provider that
10 the provider is in compliance with section 507F.7. If the
11 third-party provider fails to provide written certification to
12 the licensee, the licensee shall comply with section 507F.7.
13 The computation of the licensee's deadlines pursuant to section
14 507F.7 shall begin on the business day after the date on
15 which the licensee's third-party service provider notifies
16 the licensee of a cybersecurity event, or the date on which
17 the licensee has actual knowledge of the cybersecurity event,
18 whichever date is earlier.

19 2. This section shall not be construed to prohibit or
20 abrogate an agreement between a licensee and another licensee,
21 a third-party service provider, or any other party for the
22 other licensee, third-party service provider, or other party to
23 execute the requirements under section 507F.6 or section 507F.7
24 on behalf of the licensee.

25 Sec. 10. NEW SECTION. 507F.10 Cybersecurity event
26 reinsurers.

27 1. If a cybersecurity event involves nonpublic information
28 used by, or that is in the possession, custody, or control
29 of, a licensee that is acting as an assuming insurer and that
30 does not have a direct contractual relationship with consumers
31 affected by the cybersecurity event, the assuming insurer
32 shall notify each of the assuming insurer's affected ceding
33 insurers and the commissioner of the assuming insurer's state
34 of domicile within three business days of determining that a
35 cybersecurity event has occurred. A ceding insurer that has

1 a direct contractual relationship with a consumer affected by
2 the cybersecurity event shall comply with section 507F.8 and
3 the applicable provisions of section 715C.2, and all other
4 applicable notification requirements pursuant to federal or
5 state law.

6 2. If a cybersecurity event involves nonpublic information
7 that is in the possession, custody, or control of a third-party
8 service provider of a licensee that is acting as an assuming
9 insurer, the assuming insurer shall notify each of the assuming
10 insurer's affected ceding insurers and the commissioner of the
11 assuming insurer's state of domicile within three business
12 days of the date the assuming insurer receives notice from
13 the assuming insurer's third-party service provider that
14 a cybersecurity event involving nonpublic information has
15 occurred. A ceding insurer that has a direct contractual
16 relationship with a consumer affected by the cybersecurity
17 event shall comply with section 507F.8 and the applicable
18 provisions of section 715C.2, and all other applicable
19 notification requirements pursuant to federal or state law.

20 3. Notwithstanding any law to the contrary, a licensee
21 acting as an assuming insurer shall have no other notice
22 obligations related to a cybersecurity event or other data
23 breach than the notice requirements pursuant to subsections 1
24 and 2.

25 Sec. 11. NEW SECTION. 507F.11 **Cybersecurity event —**
26 **producers of record.**

27 If a cybersecurity event involves nonpublic information
28 that is in the possession, custody, or control of a licensee
29 that is an insurer, or in the possession, custody, or control
30 of the insurer's third-party service provider, and for
31 which a consumer accessed the insurer's services through an
32 independent insurance producer, the insurer shall notify the
33 insurance producer of record of each consumer affected by the
34 cybersecurity event no later than the date on which notice is
35 provided to affected consumers pursuant to section 507F.7. An

1 insurer shall not be required to notify an insurance producer
2 that is not authorized by law or contract to sell, solicit, or
3 negotiate on behalf of the insurer, or in a circumstance in
4 which the insurer does not have current contact information for
5 the producer of record for a specific affected consumer.

6 Sec. 12. NEW SECTION. 507F.12 Confidentiality.

7 1. Documents, materials, and other information in the
8 control or possession of the commissioner that are furnished
9 by a licensee, or by an employee or agent of the licensee
10 acting on behalf of the licensee, or that are obtained by
11 the commissioner in an investigation or examination, shall
12 be confidential by law and privileged, shall not constitute
13 a public record under chapter 22, shall not be subject to
14 subpoena or discovery, and shall not be admissible as evidence
15 in a private civil action. The commissioner, however, shall
16 be authorized to use the documents, materials, and other
17 information in the furtherance of a regulatory or legal action
18 brought as part of the commissioner's official duties. The
19 commissioner shall not otherwise make the documents, materials,
20 and other information public without the prior written consent
21 of the licensee.

22 2. The commissioner, or an individual who receives
23 documents, materials, or other information under the authority
24 of the commissioner, shall not be permitted or required to
25 testify in a private civil action concerning any documents,
26 materials, or other information subject to subsection 1.

27 3. In order to assist in the performance of the
28 commissioner's duties under this chapter, the commissioner may:

29 a. Share documents, materials, and other information,
30 including documents, materials, and other information subject
31 to subsection 1, with state, federal, and international
32 regulatory agencies; the national association of insurance
33 commissioners, its affiliates and subsidiaries; and with
34 state, federal, and international law enforcement authorities,
35 provided that the recipient certifies in writing that the

1 recipient will maintain the confidentiality or privileged
2 status of any documents, materials, or other information to
3 which confidentiality or privileged status applies.

4 *b.* Receive documents, materials, and other information,
5 including confidential and privileged documents, materials,
6 and other information from the national association of
7 insurance commissioners, its affiliates and subsidiaries;
8 and regulatory and law enforcement officials of foreign and
9 domestic jurisdictions. The commissioner shall maintain as
10 confidential or privileged any document, material, or other
11 information received by the commissioner that is confidential
12 or privileged, or that is received with notice or the
13 understanding that it is confidential or privileged, under the
14 laws of the jurisdiction that is the source of the document,
15 material, or other information.

16 *c.* Share documents, materials, or other information subject
17 to subsection 1 with a third-party consultant or vendor
18 provided that the third-party consultant or vendor certifies
19 in writing that the consultant or vendor will maintain the
20 confidentiality and privileged status of the document,
21 material, or other information.

22 *d.* Enter into an agreement governing the sharing and use of
23 documents, materials, or other information that is consistent
24 with this subsection.

25 4. No waiver of an applicable privilege or claim of
26 confidentiality in a document, material, or other information
27 shall occur as a result of disclosure of the document,
28 material, or other information to the commissioner under
29 this chapter, or as a result of the sharing of the document,
30 material, or other information as authorized under this
31 section.

32 5. This chapter shall not prohibit the commissioner from
33 releasing final, adjudicated actions that are open to public
34 inspection pursuant to chapter 22, to a database or other
35 clearinghouse service maintained by the national association of

1 insurance commissioners, or its affiliates and subsidiaries.

2 6. Documents, materials, and other information received
3 by the commissioner under this chapter and shared pursuant to
4 subsection 3, shall be confidential by law and privileged,
5 shall not constitute a public record under chapter 22, shall
6 not be subject to subpoena or discovery, and shall not be
7 admissible as evidence in a private civil action.

8 7. Ownership of documents, materials, and other information
9 shared under this chapter with the national association of
10 insurance commissioners, its affiliates and subsidiaries,
11 or a third-party consultant or vendor, remains with the
12 commissioner, and use of the documents, materials, and
13 other information by the national association of insurance
14 commissioners, its affiliates and subsidiaries, or a
15 third-party consultant or vendor is subject to the direction of
16 the commissioner.

17 Sec. 13. NEW SECTION. 507F.13 **Applicability.**

18 1. This chapter shall not apply to a licensee that is
19 subject to, and in compliance with, the Health Insurance
20 Portability and Accountability Act. The licensee shall
21 annually submit to the commissioner a written certification of
22 the licensee's compliance with HIPAA.

23 2. A licensee shall have one hundred eighty days from the
24 date the licensee no longer qualifies for exemption under
25 subsection 1 to comply with this chapter.

26 Sec. 14. NEW SECTION. 507F.14 **Penalties.**

27 A licensee that violates this chapter shall be subject to
28 penalties pursuant to section 505.7A and chapter 507B.

29 Sec. 15. NEW SECTION. 507F.15 **Rules and enforcement.**

30 1. The commissioner may adopt rules pursuant to chapter 17A
31 as necessary to administer this chapter.

32 2. The commissioner may take any enforcement action under
33 the commissioner's authority to enforce compliance with this
34 chapter.

35 Sec. 16. NEW SECTION. 507F.16 **Severability.**

1 If any provision of this chapter or its application to any
2 person or circumstance is held invalid, the invalidity shall
3 not affect other provisions or applications of this chapter
4 which can be given effect without the invalid provision or
5 application, and to this end the provisions of this chapter are
6 severable.

7 Sec. 17. NEW SECTION. 507F.17 **Effective date.**

8 This chapter takes effect January 1, 2022.

9 EXPLANATION

10 The inclusion of this explanation does not constitute agreement with
11 the explanation's substance by the members of the general assembly.

12 This bill relates to the exclusive state standards for data
13 security, and investigations and notifications of cybersecurity
14 events, for certain licensees under the jurisdiction of the
15 commissioner of insurance. The bill is based on the national
16 association of insurance commissioners' (NAIC) insurance data
17 security model law.

18 "Licensee" is defined in the bill as a person licensed,
19 authorized to operate, or registered, or required to be
20 licensed, authorized to operate, or registered pursuant to the
21 insurance laws of this state. "Licensee" does not include
22 a purchasing group or a risk retention group chartered and
23 licensed in a state other than this state, or a person acting
24 as an assuming insurer that is domiciled in another state or
25 jurisdiction. The bill does not create or imply a private
26 cause of action for a violation of its provisions, and does not
27 curtail a private cause of action that would otherwise exist in
28 the absence of the bill.

29 The bill requires licensees to develop, implement, and
30 maintain a comprehensive written information security program
31 (program) based on the licensee's risk assessment (assessment)
32 conducted pursuant to the bill. Licensees must comply with
33 the program requirements no later than January 1, 2023. The
34 program must safeguard the licensee's nonpublic information
35 and information system. "Information system" is defined in

1 the bill as a discrete set of electronic information resources
2 organized for the collection, processing, maintenance,
3 use, sharing, dissemination, or disposition of electronic
4 information, and any specialized system such as an industrial
5 or process controls system, a telephone switching and private
6 branch exchange system, or an environmental control system.
7 "Nonpublic information" is also defined in the bill. Certain
8 licensees and other persons are exempt from the program
9 requirement as detailed in the bill. The bill requires a
10 licensee's program to protect the security and confidentiality
11 of nonpublic information and the security of the information
12 system, to protect against threats or hazards to the security
13 or integrity of nonpublic information and the information
14 system, to protect against unauthorized access to or the use of
15 nonpublic information, to minimize the likelihood of harm to
16 consumers, and to define and periodically reevaluate a schedule
17 for the retention and destruction of nonpublic information.

18 A licensee's assessment must designate one or more
19 employees, an affiliate, or an outside vendor to act on
20 behalf of the licensee and to have responsibility for the
21 program; identify reasonably foreseeable internal or external
22 threats that may result in unauthorized access, transmission,
23 disclosure, misuse, alteration, or destruction of nonpublic
24 information, including nonpublic information that is accessible
25 to, or held by, a third-party service provider; assess the
26 probability of and the potential damage caused by identified
27 threats; and assess the sufficiency of policies, procedures,
28 information systems, and other safeguards in place to manage
29 identified threats. The assessment must include consideration
30 of threats identified in each relevant area of the licensee's
31 operations.

32 Based on a licensee's assessment, the bill requires
33 the licensee to design the program to mitigate identified
34 risks, to determine and implement appropriate security
35 measures, to include cybersecurity risks in the licensee's

1 enterprise-wide risk management process, to maintain knowledge
2 and understanding of emerging threats or vulnerabilities, to
3 utilize reasonable security measures when sharing information,
4 and to provide the licensee's personnel with cybersecurity
5 awareness training.

6 If a licensee has a board of directors, the bill directs
7 the board to require the licensee's executive management
8 or its delegates to develop, implement, and maintain the
9 licensee's program, and to provide an annual report to the
10 board that documents the information specified in the bill.

11 If a licensee's executive management delegates any of its
12 responsibilities, it must oversee the delegate's development,
13 implementation, and maintenance of the licensee's program.

14 As part of a licensee's program, the bill requires the
15 licensee to establish a written incident response plan (plan)
16 designed to respond to, and recover from, a cybersecurity
17 event that compromises the confidentiality, integrity, or
18 availability of nonpublic information in the licensee's
19 possession or information systems; or that compromises
20 the continuing functionality of the licensee's operations.
21 The plan must address all criteria specified in the bill.
22 "Cybersecurity event" is defined in the bill as an event
23 resulting in unauthorized access to, or the disruption or
24 misuse of, an information system or of nonpublic information
25 stored on an information system. "Cybersecurity event" does
26 not include the unauthorized acquisition of encrypted nonpublic
27 information if the encryption, process, or key is not also
28 acquired, released, or used without authorization; or an
29 event for which a licensee has determined that the nonpublic
30 information accessed by an unauthorized person has not been
31 used or released, and the nonpublic information has been
32 returned or destroyed. Insurers domiciled in this state must
33 submit an annual certification to the commissioner that the
34 insurer is in compliance with the plan requirements.

35 The bill requires a licensee to exercise due diligence in

1 the selection of a third-party service provider (provider),
2 to conduct oversight of all provider arrangements, and to
3 require all providers to implement appropriate administrative,
4 technical, and physical measures to protect and secure
5 the information systems and nonpublic information that are
6 accessible to, or held by, the provider. Licensees must
7 comply with these requirements no later than January 1, 2024.
8 "Third-party service provider" is defined in the bill as a
9 person that is not a licensee that contracts with a licensee
10 to maintain, process, store, or is otherwise permitted access
11 to nonpublic information through the person's provision of
12 services to the licensee.

13 If a licensee discovers that a cybersecurity event has
14 occurred, or that a cybersecurity event may have occurred,
15 the licensee, or the outside vendor or provider the licensee
16 has designated to act on behalf of the licensee, must conduct
17 a prompt investigation of the event as detailed in the bill.
18 If a licensee learns that a cybersecurity event has occurred,
19 or may have occurred, in an information system maintained by
20 a provider of the licensee, the licensee must complete the
21 same type of investigation, or confirm and document that the
22 provider has completed such an investigation. A licensee
23 must maintain all records and documentation related to the
24 licensee's investigation for a minimum of five years from the
25 date of the cybersecurity event.

26 A licensee is required to notify the commissioner no later
27 than three business days from the date of the licensee's
28 confirmation of a cybersecurity event if the licensee is an
29 insurer who is domiciled in this state, or is a producer whose
30 home state is this state, and state or federal law requires
31 notice to a government body, self-regulatory agency, or other
32 supervisory body. A licensee must also notify the commissioner
33 if the cybersecurity event has a reasonable likelihood of
34 causing material harm to a consumer, or to a material part of
35 the normal business, operations, or security of the licensee;

1 or the licensee reasonably believes that nonpublic information
2 compromised by the cybersecurity event involves 250 or more
3 consumers and state or federal law requires notice to a
4 government body, self-regulatory agency, or other supervisory
5 body. The licensee must provide the commissioner with
6 the information specified in the bill and has a continuing
7 obligation to update and supplement the information as material
8 changes to the information occur.

9 In the event of a cybersecurity event involving nonpublic
10 information, the licensee must notify consumers as detailed
11 in the bill. A licensee that has to provide notification to
12 more than 500 consumers must also give written notice to the
13 director of the consumer protection division of the office of
14 the attorney general within five business days of the date
15 the first notice of the cybersecurity event is provided to an
16 affected consumer. The bill also details the requirements
17 for cybersecurity event notifications related to providers,
18 reinsurers, and producers of record.

19 The bill details confidentiality and privilege as applied
20 to documents, materials, or other information furnished by a
21 licensee, or that are obtained by the commissioner pursuant to
22 an investigation or examination, and that are in the control
23 or possession of the commissioner. The bill details which
24 documents, materials, or other information do not constitute
25 a public record under Code chapter 22; are not subject to
26 subpoena and discovery; and are not admissible in a private
27 civil action. The bill also describes how the documents,
28 materials, and other information may be shared or used by the
29 commissioner.

30 The bill does not apply to a licensee that is subject to,
31 and in compliance with, the Health Insurance Portability and
32 Accountability Act of 1996 (HIPAA). The licensee must submit
33 an annual written certification to the commissioner of the
34 licensee's compliance with HIPAA.

35 A licensee that violates the bill shall be subject to

1 penalties pursuant to Code section 505.7A and Code chapter
2 507B.

3 The commissioner may adopt rules to administer the bill
4 and may take any enforcement action under the commissioner's
5 authority to enforce compliance with the bill.

6 If any provision of the bill, or its application to any
7 person or circumstance is held invalid, the invalidity does not
8 affect other provisions or applications of the bill which can
9 be given effect without the invalid provision or application.

10 The bill takes effect January 1, 2022.