**House File 719 - Enrolled**

House File 719

AN ACT
RELATING TO STANDARDS FOR DATA SECURITY, AND INVESTIGATIONS AND
   NOTIFICATIONS OF CYBERSECURITY EVENTS, FOR CERTAIN LICENSEES
   UNDER THE JURISDICTION OF THE COMMISSIONER OF INSURANCE,
   MAKING PENALTIES APPLICABLE, AND INCLUDING EFFECTIVE DATE
   PROVISIONS.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

   Section 1. NEW SECTION. **507F.1 Title.**
   This chapter may be cited as the "*Insurance Data Security
Act*".
   Sec. 2. NEW SECTION. **507F.2 Purpose and scope.**
   1. Notwithstanding any provision of law to the contrary,
this chapter establishes the exclusive state standards for
data security, and the investigation and notification of
cybersecurity events, applicable to licensees.
   2. This chapter shall not be construed to create or imply
a private cause of action for a violation of its provisions,
and shall not be construed to curtail a private cause of action
that otherwise exists in the absence of this chapter.
   Sec. 3. NEW SECTION. **507F.3 Definitions.**
   As used in this chapter, unless the context otherwise
requires:
   1. "*Authorized individual*" means an individual known to
and screened by a licensee and determined to be necessary and
appropriate to have access to nonpublic information held by the
licensee and the licensee's information system.

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

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

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

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

*b.* An event for which a licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released, and the nonpublic information has been returned or destroyed.

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

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

7. *"Gramm-Leach-Bliley Act"* means the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801 et seq., including amendments thereto and regulations promulgated thereunder.

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

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

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

11. *"Information system"* means a discrete set of electronic information resources organized for the collection, processing,

maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information, and any specialized system such as an industrial or process controls system, a telephone switching and private branch exchange system, or an environmental control system.

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

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

14. *"Multi-factor authentication"* means authentication through verification of at least two of the following types of authentication factors:

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

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

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

15. *"Nonpublic information"* means electronic information that is not publicly available information and that is any of the following:

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

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

(1) A social security number.

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

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

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

(5) A biometric record.

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

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

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

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

16. *"Person"* means an individual or a nongovernmental entity, including but not limited to a nongovernmental partnership, corporation, branch, agency, or association.

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

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

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

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

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

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

1. *a.* Commensurate with the size and complexity of a licensee, the nature and scope of a licensee's activities including the licensee's use of third-party service providers,

and the sensitivity of nonpublic information used by the licensee or that is in the licensee's possession, custody, or control, the licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment conducted pursuant to subsection 3.

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

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

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

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

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

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

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

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

*a.* Protect the security and confidentiality of nonpublic information and the security of the licensee's information system.

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

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

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

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

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

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

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

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

(1) Employee training and management.

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

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

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

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

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

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

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

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable the licensee to achieve

its business purposes in accordance with the data, personnel,
devices, systems, and facilities relative importance to the
licensee's business objectives and risk strategy.

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

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

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

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

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

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

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

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

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

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

*d.* Maintain knowledge and understanding of emerging threats
or vulnerabilities and utilize reasonable security measures,

relative to the character of the sharing and the type of
information being shared, when sharing information.

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

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

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

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

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

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

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

    6. A licensee shall monitor, evaluate, and adjust the
licensee's information security program consistent with
relevant changes in technology, the sensitivity of the
licensee's nonpublic information, changes to the licensee's
information systems, internal or external threats to the
licensee's nonpublic information, and the licensee's changing
business arrangements, including but not limited to mergers and

acquisitions, alliances and joint ventures, and outsourcing
arrangements.

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

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

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

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

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

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

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

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

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

or the commissioner's representative, upon request of the
commissioner.

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

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

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

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

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

1. If a licensee discovers that a cybersecurity event has
occurred, or that a cybersecurity event may have occurred, the
licensee, or the outside vendor or third-party service provider
the licensee has designated to act on behalf of the licensee,
shall conduct a prompt investigation of the event.

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

*a.* Confirm that a cybersecurity event has occurred.

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

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

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

3. If a licensee learns that a cybersecurity event has
occurred, or may have occurred, in an information system
maintained by a third-party service provider of the licensee,

the licensee shall complete an investigation in compliance with this section, or confirm and document that the third-party service provider has completed an investigation in compliance with this section.

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

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

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

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

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

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

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

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

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

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

time of the notification:

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

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

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

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

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

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

   *g.* A description of the specific types of nonpublic information that were lost, stolen, or breached.

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

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

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

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

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

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

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

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

1. In the event of a cybersecurity event involving nonpublic
information a licensee shall comply with the notification
requirements pursuant to section 715C.2, and all other
applicable notification requirements pursuant to federal or
state law.

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

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

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

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

Sec. 10. NEW SECTION. **507F.10 Cybersecurity event
reinsurers.**

1. If a cybersecurity event involves nonpublic information
used by, or that is in the possession, custody, or control
of, a licensee that is acting as an assuming insurer and that

does not have a direct contractual relationship with consumers
affected by the cybersecurity event, the assuming insurer
shall notify each of the assuming insurer's affected ceding
insurers and the commissioner of the assuming insurer's state
of domicile within three business days of determining that a
cybersecurity event has occurred. A ceding insurer that has a
direct contractual relationship with a consumer affected by the
cybersecurity event shall comply with the applicable provisions
of section 715C.2, and all other applicable notification
requirements pursuant to federal or state law.

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

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

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

If a cybersecurity event involves nonpublic information
that is in the possession, custody, or control of a licensee
that is an insurer, or in the possession, custody, or control
of the insurer's third-party service provider, and for
which a consumer accessed the insurer's services through an
independent insurance producer, the insurer shall notify the
insurance producer of record of each consumer affected by the
cybersecurity event no later than the date on which notice is

provided to affected consumers pursuant to section 507F.7. An
insurer shall not be required to notify an insurance producer
that is not authorized by law or contract to sell, solicit, or
negotiate on behalf of the insurer, or in a circumstance in
which the insurer does not have current contact information for
the producer of record for a specific affected consumer.

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

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

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

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

*a.* Share documents, materials, and other information,
including documents, materials, and other information subject
to subsection 1, with state, federal, and international
regulatory agencies; the national association of insurance
commissioners, its affiliates and subsidiaries; and with
state, federal, and international law enforcement authorities,
provided that the recipient certifies in writing that the
recipient will maintain the confidentiality or privileged
status of any documents, materials, or other information to
which confidentiality or privileged status applies.

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

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

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

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

5. This chapter shall not prohibit the commissioner from
releasing final, adjudicated actions that are open to public
inspection pursuant to chapter 22, to a database or other
clearinghouse service maintained by the national association of
insurance commissioners, or its affiliates and subsidiaries.

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

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

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

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

2. This chapter shall not apply to a licensee that is owned or controlled by a federally insured depository institution that is subject to, and in compliance with, the Gramm-Leach-Bliley Act or comparable federal law and corresponding regulations.

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

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

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

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

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

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

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

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

Sec. 17.  EFFECTIVE DATE.  This Act takes effect January 1, 2022.

_____          _____
PAT GRASSLEY                             JAKE CHAPMAN
Speaker of the House                     President of the Senate


I hereby certify that this bill originated in the House and is known as House File 719, Eighty-ninth General Assembly.


                                         _____
                                         MEGHAN NELSON
                                         Chief Clerk of the House


Approved _____, 2021           _____
                                         KIM REYNOLDS
                                         Governor