CHAPTER 26.1-02.2
INSURANCE DATA SECURITY

26.1-02.2-01. Definitions.

As used in this chapter:

1. "Authorized individual" means an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and the licensee's information systems.
2. "Commissioner" means the insurance commissioner.
3. "Consumer" means an individual, including an applicant, policyholder, insured, beneficiary, claimant, and 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, disruption, or misuse of, an information system or nonpublic information stored on the information system. The term does not include:
   a. The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization; or
   b. An event the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.
5. "Department" means the insurance department.
6. "Encrypted" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.
7. "Information security program" means the administrative, technical, and physical safeguards a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.
8. "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, as well as any specialized system, including industrial or process controls systems, telephone switching, private branch exchange systems, and environmental control systems.
9. "Licensee" means any person licensed, authorized to operate, registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state. The term does not include a purchasing group or a risk retention group chartered and licensed in another state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.
10. "Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors:
    a. Knowledge factors, including a password;
    b. Possession factors, including a token or text message on a mobile phone; or
    c. Inherence factors, including a biometric characteristic.
11. "Nonpublic information" means electronic information that is not publicly available information and is:
    a. Any information concerning a consumer which can be used to identify the consumer because of name, number, personal mark, or other identifier in combination with any one or more of the following data elements:
       (1) Social security number;
       (2) Driver's license number or nondriver identification card number;
       (3) Financial account number or credit or debit card number;
       (4) Any security code, access code, or password that would permit access to a consumer's financial account; or
       (5) Biometric records.
    b. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer which can be used to identify a particular consumer and relates to:

(1) The past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family;
(2) The provision of health care to any consumer; or
(3) Payment for the provision of health care to any consumer.

12. "Person" means any individual or any nongovernmental entity, including any nongovernmental partnership, corporation, branch, agency, or association.
13. "Publicly available information" means any information a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or disclosures to the general public which are required to be made by federal, state, or local law. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:
    a. The information is of the type available to the general public; and
    b. Whether a consumer can direct the information not be made available to the general public and, if so, that the consumer has not done so.
14. "Risk assessment" means the risk assessment that each licensee is required to conduct under section 26.1-02.2-03.
15. "Third-party service provider" means a person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, store, or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

26.1-02.2-02. Exclusive regulation.

Notwithstanding any other provision of law, this chapter establishes the exclusive state standards applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the commissioner.

26.1-02.2-03. Information security program.

1. Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including the licensee's use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.
2. A licensee's information security program must be designed to:
    a. Protect the security and confidentiality of nonpublic information and the security of the information system;
    b. Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;
    c. Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer; and
    d. Define and periodically re-evaluate a schedule for retention of nonpublic information and a mechanism for destruction if no longer needed.
3. The licensee shall:
    a. Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee which is responsible for the information security program;
    b. Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information accessible to, or held by, third-party service providers;
    c. Assess the likelihood and potential damage of any threats, taking into consideration the sensitivity of the nonpublic information;

d. Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage any threats, including consideration of threats in each relevant area of the licensee's operations, including:
   (1) Employee training and management;
   (2) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and
   (3) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and
e. Implement information safeguards to manage the threats identified in the licensee's ongoing assessment and assess the effectiveness of the safeguards' key controls, systems, and procedures on an annual basis.

4. Based on the licensee's risk assessment, the licensee shall:
   a. Design the information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including the licensee's use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control.
   b. Determine which security measures as provided under this subdivision are appropriate and implement the security measures:
      (1) Place access controls on information systems, including controls to authenticate and permit access only to an authorized individual to protect against the unauthorized acquisition of nonpublic information;
      (2) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with the business' relative importance to business objectives and the organization's risk strategy;
      (3) Restrict physical access to nonpublic information only to an authorized individual;
      (4) Protect by encryption or other appropriate means, all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;
      (5) Adopt secure development practices for in-house developed applications utilized by the licensee;
      (6) Modify the information system in accordance with the licensee's information security program;
      (7) Utilize effective controls, which may include multi-factor authentication procedures for employees 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 normal operations and obligations of the licensee;
      (10) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, including fire and water damage or other catastrophes or technological failures; and
      (11) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.
   c. Include cybersecurity risks in the licensee's enterprise risk management process.
   d. Stay informed regarding emerging threats or vulnerabilities and use reasonable security measures if sharing information relative to the character of the sharing and the type of information shared.

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

5. If the licensee has a board of directors, the board or an appropriate committee of the board at a minimum shall:
   a. Require the licensee's executive management or the licensee's delegates to develop, implement, and maintain the licensee's information security program.
   b. Require the licensee's executive management or the licensee's delegates to report the following information in writing on an annual basis:
      (1) The overall status of the information security program and the licensee's compliance with the provisions of this chapter; and
      (2) Material matters related to the information security program, addressing issues, including risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events, or violations, and management's responses and recommendations for changes in the information security program.
   c. If executive management delegates any responsibilities under this section, the executive management delegates shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors.
6. A licensee shall exercise due diligence in selecting its third-party service provider; and a licensee shall require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information accessible to, or held by, the third-party service provider.
7. The licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, including mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.
8. As part of the licensee's information security program, a licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in the licensee's possession. The incident response plan must include the licensee's plan to recover the licensee's information systems and restore continuous functionality of any aspect of the licensee's business or operations.
9. A licensee's incident response plan must address:
   (1) The internal process for responding to a cybersecurity event;
   (2) The goals of the incident response plan;
   (3) The definition of clear roles, responsibilities, and levels of decisionmaking authority;
   (4) External and internal communications and information sharing;
   (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
   (6) Documentation and reporting regarding cybersecurity events and related incident response activities; and
   (7) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.
10. Annually, an insurer domiciled in this state shall submit to the commissioner, a written statement by April fifteenth, certifying the insurer is in compliance with the requirements set forth in this section. An insurer shall maintain for examination by the department all records, schedules, and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address the areas,

systems, or processes. The documentation must be available for inspection by the commissioner.

26.1-02.2-04. Investigation of a cybersecurity event.

1. If a licensee learns a cybersecurity event has or may have occurred, the licensee, an outside vendor, or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.
2. During the investigation, the licensee or an outside vendor or service provider designated to act on behalf of the licensee, at a minimum shall:
   a. Determine whether a cybersecurity event has occurred;
   b. Assess the nature and scope of the cybersecurity event;
   c. Identify any nonpublic information that may have been involved in the cybersecurity event; and
   d. Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.
3. If a licensee learns a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee shall complete the requirements provided under subsection 2 or confirm and document that the third-party service provider has completed the requirements.
4. The licensee shall maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event and shall produce the records upon demand of the commissioner.

26.1-02.2-05. Notification of a cybersecurity event.

1. A licensee shall notify the commissioner as promptly as possible, but no later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred if:
   a. This state is the licensee's state of domicile, in the case of an insurer, or this state is the licensee's home state, in the case of a producer as defined in chapter 26.1-26, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or reasonable likelihood of materially harming any material part of the normal operations of the licensee; or
   b. The licensee reasonably believes the nonpublic information involved is of two hundred fifty or more consumers residing in this state and is:
      (1) A cybersecurity event impacting the licensee for which notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law; or
      (2) A cybersecurity event that has a reasonable likelihood of materially harming any consumer residing in this state or materially harming any part of the normal operations of the licensee.
2. The licensee shall provide the notice required under this section in electronic form as directed by the commissioner. The licensee shall update and supplement the initial and any subsequent notifications to the commissioner regarding material changes to previously provided information relating to the cybersecurity event. The licensee's notice required under this section must include:
   a. The date of the cybersecurity event;
   b. Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any;
   c. How the cybersecurity event was discovered;
   d. Whether any lost, stolen, or breached information has been recovered and if so, how;
   e. The identity of the source of the cybersecurity event;

f. Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when the notification was provided;
g. Description of the specific types of information acquired without authorization. Specific types of information means particular data elements, including medical information, financial information, or any other information allowing identification of the consumer;
h. The period during which the information system was compromised by the cybersecurity event;
i. The total number of consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update the estimate with a subsequent report to the commissioner pursuant to this section;
j. The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
k. Description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;
l. A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and
m. Name of a contact person that is both familiar with the cybersecurity event and authorized to act for the licensee.

3. The licensee shall comply with chapter 51-30, as applicable, and provide a copy of the notice sent to consumers to the commissioner, when a licensee is required to notify the commissioner under subsection 1.
4. In the case of a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat the event in accordance with subsection 1 unless the third-party service provider provides the notice required under chapter 26.1-02.2 to the commissioner.
   a. The computation of licensee's deadlines under this subsection begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.
   b. Nothing in this chapter prevents or abrogates an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill any of the investigation requirements imposed under section 26.1-02.2-04 or notice requirements imposed under subsection 1.
5. If a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or 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 the affected consumers, the assuming insurer shall notify the insurer's affected ceding insurers and the commissioner of the insurer's state of domicile within three business days of making the determination that a cybersecurity event has occurred. The ceding insurer that has a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under chapter 51-30 and any other notification requirements relating to a cybersecurity event imposed under subsection 1.
6. If a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is an assuming insurer, the assuming insurer shall notify the insurer's affected ceding insurers and the commissioner of the insurer's state of domicile within three business days of receiving notice from its third-party service provider that a cybersecurity event has occurred. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under chapter 51-30 and

any other notification requirements relating to a cybersecurity event imposed under subsection 1.

7. Any licensee acting as assuming insurer does not have any other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.
8. If a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that is an insurer or the insurer's third-party service provider for which a consumer accessed the insurer's services through an independent insurance producer, and for which consumer notice is required by chapter 51-30, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event no later than the time at which notice is provided to the affected consumers. The insurer is excused from the obligation imposed under this subsection for any producers that are not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and those instances in which the insurer does not have the current producer of record information for an individual consumer.

26.1-02.2-06. Power of commissioner.

1. The commissioner may examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this chapter. This power is in addition to the powers the commissioner has under chapter 26.1-03. Any investigation or examination must be conducted pursuant to chapter 26.1-03.
2. If the commissioner has reason to believe a licensee has been or is engaged in conduct in this state which violates this chapter, the commissioner may take action that is necessary or appropriate to enforce the provisions of this chapter.

26.1-02.2-07. Confidentiality.

1. Any documents, materials, or other information in the control or possession of the department which are furnished by a licensee, or an employee or agent thereof acting on behalf of a licensee pursuant to this chapter, or that are obtained by the commissioner in an investigation or examination pursuant to section 26.1-02.2-06 are confidential, not subject to chapter 44-04, not subject to subpoena, and are not subject to discovery or admissible in evidence in any private civil action. The commissioner may use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the commissioner's duties. The commissioner may not otherwise make the documents, materials, or other information public without the prior written consent of the licensee.
2. The commissioner or any person that received documents, materials, or other information while acting under the authority of the commissioner may not be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to subsection 1.
3. In order to assist in the performance of the commissioner's duties the commissioner:
    a. May share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection 1, with other state, federal, and international regulatory agencies, with the national association of insurance commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information;
    b. May receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the national association of insurance commissioners, its affiliates or subsidiaries, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material, or information 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 information;

c. May share documents, materials, or other information subject to this section, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information; and

d. May enter agreements governing sharing and use of information consistent with this subsection.

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

5. Documents, materials, or other information in the possession or control of the national association of insurance commissioners or a third-party consultant or vendor pursuant to this chapter are confidential, not subject to chapter 44-04, not subject to subpoena, and not subject to discovery or admissible in evidence in any private civil action.

26.1-02.2-08. Exceptions.

1. The following exceptions apply to this chapter:

a. A licensee with less than five million dollars in gross revenue or less than ten million dollars in year-end assets is exempt from section 26.1-02.2-03.

b. During the period beginning on August 1, 2021, and ending on July 31, 2023, a licensee with fewer than fifty employees, including independent contractors and employees of affiliated companies having access to nonpublic information used by the licensee or in the licensee's possession, custody, or control, is exempt from section 26.1-02.2-03.

c. After July 31, 2023, a licensee with fewer than twenty-five employees, including independent contractors and employees of affiliated companies having access to nonpublic information used by the licensee or in the licensee's possession, custody, or control is exempt from section 26.1-02.2-03.

d. A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, title 45, Code of Federal Regulations, parts 160 and 164, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 [Pub. L. 104-191], and the federal Health Information Technology for Economic and Clinical Health Act [Pub. L. 111-5], and which maintains nonpublic information concerning a consumer in the same manner as protected health information is deemed to comply with the requirements of this chapter except for the commissioner notification requirements under subsections 1 and 2 of section 26.1-02.2-05.

e. An employee, agent, representative, or designee of a licensee, that also is a licensee, is exempt from section 26.1-02.2-03 and is not required to develop an information security program to the extent the employee, agent, representative, or designee is covered by the information security program of the other licensee.

2. If a licensee ceases to qualify for an exception, the licensee has one hundred eighty days to comply with this chapter.

26.1-02.2-09. Penalties.

In the case of a violation of this chapter, a licensee may be penalized in accordance with section 26.1-01-03.3.

26.1-02.2-10. Rules and regulations.

The commissioner may adopt reasonable rules necessary for the implementation of this chapter.

26.1-02.2-11. Implementation dates.

A licensee shall implement:

1. Subsections 1, 2, 3, 4, 5, 8, and 9 of section 26.1-02.2-03 no later than August 1, 2022; and
2. Subsections 6 and 7 of section 26.1-02.2-03 no later than August 1, 2023.