State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-SECOND SESSION

H. F. No. 1913

03/04/2021 Authored by Elkins
The bill was read for the first time and referred to the Committee on Commerce Finance and Policy
03/22/2021 Adoption of Report: Placed on the General Register as Amended
Read for the Second Time
04/12/2021 Calendar for the Day, Amended
Read Third Time as Amended
Passed by the House as Amended and transmitted to the Senate to include Floor Amendments

A bill for an act

relating to insurance; establishing an Insurance Data Security Law; proposing coding for new law in Minnesota Statutes, chapter 60A; repealing Minnesota Statutes 2020, sections 60A.98; 60A.981; 60A.982.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[60A.985] DEFINITIONS.**

Subdivision 1. **Terms.** As used in sections 60A.985 to 60A.9857, the following terms have the meanings given.

Subd. 2. **Authorized individual.** "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 its information systems.

Subd. 3. **Consumer.** "Consumer" means an individual, including but not limited to 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.

Subd. 4. **Cybersecurity event.** "Cybersecurity event" means an event resulting in unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on an information system.

Cybersecurity event does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization.

Cybersecurity event does not include an event with regard to which 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.

Subd. 5. **Encrypted.** "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

Subd. 6. **Information security program.** "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.

Subd. 7. **Information system.** "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of nonpublic electronic information, as well as any specialized system such as industrial or process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

Subd. 8. **Licensee.** "Licensee" means any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered by the Department of Commerce or the Department of Health under chapters 59A to 62M and 62Q to 79A.

Subd. 9. **Multifactor authentication.** "Multifactor authentication" means authentication through verification of at least two of the following types of authentication factors:

(1) knowledge factors, such as a password;

(2) possession factors, such as a token or text message on a mobile phone; or

(3) inherence factors, such as a biometric characteristic.

Subd. 10. **Nonpublic information.** "Nonpublic information" means electronic information that is not publicly available information and is:

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

(i) Social Security number;

(ii) driver's license number or nondriver identification card number;

(iii) financial account number, credit card number, or debit card number;

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

(v) biometric records; or

(2) 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 that can be used to identify a particular consumer and that relates to:

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

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

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

Subd. 11. **Person.** "Person" means any individual or any nongovernmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency, or association.

Subd. 12. **Publicly available information.** "Publicly available information" means any 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; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law.

For the 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 taken steps to determine:

(1) that the information is of the type that is available to the general public; and

(2) whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.

Subd. 13. **Risk assessment.** "Risk assessment" means the risk assessment that each licensee is required to conduct under section 60A.9853, subdivision 3.

Subd. 14. **State.** "State" means the state of Minnesota.

Subd. 15. **Third-party service provider.** "Third-party service provider" means a person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, or store nonpublic information, or is otherwise permitted access to nonpublic information through its provision of services to the licensee.

Sec. 2. **[60A.9851] INFORMATION SECURITY PROGRAM.**

Subdivision 1. **Implementation of an information security program.** Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its 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 and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

Subd. 2. **Objectives of an information security program.** A licensee's information security program shall be designed to:

(1) protect the security and confidentiality of nonpublic information and the security of the information system;

(2) protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

(3) protect against unauthorized access to, or use of, nonpublic information, and minimize the likelihood of harm to any consumer; and

(4) define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

Subd. 3. **Risk assessment.** The licensee shall:

(1) designate one or more employees, an affiliate, or an outside vendor authorized to act on behalf of the licensee who is responsible for the information security program;

(2) identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including threats to the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;

(3) assess the likelihood and potential damage of the threats identified pursuant to clause (2), taking into consideration the sensitivity of the nonpublic information;

(4) assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(i) employee training and management;

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

(iii) detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

Subd. 4. **Risk management.** Based on its risk assessment, the licensee shall:

(1) design its 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 its 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;

(2) determine which of the following security measures are appropriate and implement any appropriate security measures:

(i) 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;

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

(iii) restrict physical access to nonpublic information to authorized individuals only;

(iv) 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;

(v) adopt secure development practices for in-house developed applications utilized by the licensee;

(vi) modify the information system in accordance with the licensee's information security program;

(vii) utilize effective controls, which may include multifactor authentication procedures for any authorized individual accessing nonpublic information;

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

(ix) 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;

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

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

(3) include cybersecurity risks in the licensee's enterprise risk management process;

(4) stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

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

Subd. 5. **Oversight by board of directors.** If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(1) require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program;

(2) require the licensee's executive management or its delegates to report in writing, at least annually, the following information:

(i) the overall status of the information security program and the licensee's compliance with this act; and

(ii) material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program; and

(3) if executive management delegates any of its responsibilities under this section, it 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.

Subd. 6. **Oversight of third-party service provider arrangements.** (a) A licensee shall exercise due diligence in selecting its third-party service provider.

(b) 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 that are accessible to, or held by, the third-party service provider.

Subd. 7. **Program adjustments.** 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, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

Subd. 8. **Incident response plan.** (a) As part of its information security program, each 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 its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations.

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

(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 decision-making 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.

Subd. 9. **Annual certification to commissioner.** (a) Subject to paragraph (b), by April 15 of each year, an insurer domiciled in this state shall certify in writing to the commissioner that the insurer is in compliance with the requirements set forth in this section. Each insurer shall maintain all records, schedules, and data supporting this certificate for a period of five

years and shall permit examination by the commissioner. 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 such areas, systems, or processes. Such documentation must be available for inspection by the commissioner.

(b) The commissioner must post on the department's website, no later than 60 days prior to the certification required by paragraph (a), the form and manner of submission required and any instructions necessary to prepare the certification.

Sec. 3. **[60A.9852] INVESTIGATION OF A CYBERSECURITY EVENT.**

Subdivision 1. **Prompt investigation.** If the licensee learns that a cybersecurity event has or may have occurred, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.

Subd. 2. **Investigation contents.** During the investigation, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall, at a minimum and to the extent possible:

(1) determine whether a cybersecurity event has occurred;

(2) assess the nature and scope of the cybersecurity event, if any;

(3) identify whether any nonpublic information was involved in the cybersecurity event and, if so, what nonpublic information was involved; and

(4) 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.

Subd. 3. **Third-party systems.** If the licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee will complete the steps listed in subdivision 2 or confirm and document that the third-party service provider has completed those steps.

Subd. 4. **Records.** 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 those records upon demand of the commissioner.

Sec. 4. **[60A.9853] NOTIFICATION OF A CYBERSECURITY EVENT.**

Subdivision 1. **Notification to the commissioner.** Each licensee shall notify the commissioner of commerce or commissioner of health, whichever commissioner otherwise regulates the licensee, without unreasonable delay but in no event later than three business days from a determination that a cybersecurity event has occurred when either of the following criteria has been met:

(1) 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 those terms are defined in chapter 60K and the cybersecurity event has a reasonable likelihood of materially harming:

(i) any consumer residing in this state; or

(ii) any part of the normal operations of the licensee; or

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

(i) a cybersecurity event impacting the licensee of 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

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

(A) any consumer residing in this state; or

(B) any part of the normal operations of the licensee.

Subd. 2. **Information; notification.** A licensee making the notification required under subdivision 1 shall provide the information in electronic form as directed by the commissioner. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning material changes to previously provided information relating to the cybersecurity event. The licensee shall provide as much of the following information as possible:

(1) date of the cybersecurity event;

(2) description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any;

(3) how the cybersecurity event was discovered;

(4) whether any lost, stolen, or breached information has been recovered and, if so, how this was done;

(5) the identity of the source of the cybersecurity event;

(6) whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided;

(7) description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer;

(8) the period during which the information system was compromised by the cybersecurity event;

(9) the number of total 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 this estimate with each subsequent report to the commissioner pursuant to this section;

(10) 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;

(11) description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur;

(12) 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

(13) name of a contact person who is familiar with the cybersecurity event and authorized to act for the licensee.

Subd. 3. **Notification to consumers.** (a) If a licensee is required to submit a report to the commissioner under subdivision 1, the licensee shall notify any consumer residing in Minnesota if, as a result of the cybersecurity event reported to the commissioner, the consumer's nonpublic information was or is reasonably believed to have been acquired by an unauthorized person, and there is a reasonable likelihood of material harm to the consumer as a result of the cybersecurity event. Consumer notification is not required for a cybersecurity event resulting from the good faith acquisition of nonpublic information by an employee or agent of the licensee for the purposes of the licensee's business, provided the nonpublic information is not used for a purpose other than the licensee's business or subject to further unauthorized disclosure. The notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach,

identify the individuals affected, and restore the reasonable integrity of the data system. The notification may be delayed to a date certain if the commissioner determines that providing the notice impedes a criminal investigation. The licensee shall provide a copy of the notice to the commissioner.

(b) For purposes of this subdivision, notice required under paragraph (a) must be provided by one of the following methods:

(1) written notice to the consumer's most recent address in the licensee's records;

(2) electronic notice, if the licensee's primary method of communication with the consumer is by electronic means or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) if the cost of providing notice exceeds $250,000, the affected class of consumers to be notified exceeds 500,000, or the licensee does not have sufficient contact information for the subject consumers, notice as follows:

(i) e-mail notice when the licensee has an e-mail address for the subject consumers;

(ii) conspicuous posting of the notice on the website page of the licensee; and

(iii) notification to major statewide media.

(c) Notwithstanding paragraph (b), a licensee that maintains its own notification procedure as part of its information security program that is consistent with the timing requirements of this subdivision is deemed to comply with the notification requirements if the licensee notifies subject consumers in accordance with its program.

(d) A waiver of the requirements under this subdivision is contrary to public policy, and is void and unenforceable.

Subd. 4. **Notice regarding cybersecurity events of third-party service providers.** (a) 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 such event as it would under subdivision 1 unless the third-party service provider provides the notice required under subdivision 1.

(b) The computation of a licensee's deadlines shall 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.

(c) Nothing in this act shall prevent or abrogate 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 60A.9854 or notice requirements imposed under this section.

Subd. 5. **Notice regarding cybersecurity events of reinsurers to insurers.** (a) In the case of a cybersecurity event involving nonpublic information that is used by the 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 its affected ceding insurers and the commissioner of its state of domicile within three business days of making the determination that a cybersecurity event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under subdivision 3 and any other notification requirements relating to a cybersecurity event imposed under this section.

(c) In the case of 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 its affected ceding insurers and the commissioner of its state of domicile within three business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(d) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under subdivision 3 and any other notification requirements relating to a cybersecurity event imposed under this section.

(e) Any licensee acting as an assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section.

Subd. 6. **Notice regarding cybersecurity events of insurers to producers of record.** (a) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that is an insurer or its third-party service provider and for which a consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected consumers no later than the time at which notice is provided to the affected consumers.

(b) The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual consumer or in those instances in which the producer of record is no longer appointed to sell, solicit, or negotiate on behalf of the insurer.

Sec. 5. **[60A.9854] POWER OF COMMISSIONER.**

(a) The commissioner of commerce or commissioner of health, whichever commissioner otherwise regulates the licensee, shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of sections 60A.985 to 60A.9857. This power is in addition to the powers which the commissioner has under section 60A.031. Any such investigation or examination shall be conducted pursuant to section 60A.031.

(b) Whenever the commissioner of commerce or commissioner of health has reason to believe that a licensee has been or is engaged in conduct in this state which violates sections 60A.985 to 60A.9857, the commissioner of commerce or commissioner of health may take action that is necessary or appropriate to enforce those sections.

Sec. 6. **[60A.9855] CONFIDENTIALITY.**

Subdivision 1. **Licensee information.** Any documents, materials, or other information in the control or possession of the department that are furnished by a licensee or an employee or agent thereof acting on behalf of a licensee pursuant to section 60A.9851, subdivision 9; section 60A.9853, subdivision 2, clauses (2), (3), (4), (5), (8), (10), and (11); or that are obtained by the commissioner in an investigation or examination pursuant to section 60A.9854 shall be classified as confidential, protected nonpublic, or both; shall not be subject to subpoena; and shall not be subject to discovery or admissible in evidence in any private civil action. However, the commissioner is authorized to 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.

Subd. 2. **Certain testimony prohibited.** Neither the commissioner nor any person who received documents, materials, or other information while acting under the authority of the commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to subdivision 1.

Subd. 3. **Information sharing.** In order to assist in the performance of the commissioner's duties under this act, the commissioner:

(1) may share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subdivision 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 that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information;

(2) 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;

(3) may share documents, materials, or other information subject to subdivision 1, 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

(4) may enter into agreements governing sharing and use of information consistent with this subdivision.

Subd. 4. **No waiver of privilege or confidentiality.** No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in subdivision 3. Any document, material, or information disclosed to the commissioner under this section about a cybersecurity event must be retained and preserved by the licensee for the time period under section 541.05, or longer if required by the licensee's document retention policy.

Subd. 5. **Certain actions public.** Nothing in sections 60A.985 to 60A.9857 shall prohibit the commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to chapter 13 to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

Subd. 6. **Classification, protection, and use of information by others.** Documents, materials, or other information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant pursuant to sections 60A.985 to 60A.9857 are classified as confidential, protected nonpublic, and privileged; are not subject to subpoena; and are not subject to discovery or admissible in evidence in a private civil action.

Sec. 7. **[60A.9856] EXCEPTIONS.**

Subdivision 1. **Generally.** The following exceptions shall apply to sections 60A.985 to 60A.9857:

(1) a licensee with fewer than 25 employees is exempt from sections 60A.9851 and 60A.9852;

(2) a licensee subject to and in compliance with the Health Insurance Portability and Accountability Act, Public Law 104-191, 110 Stat. 1936 (HIPAA), is considered to comply with sections 60A.9851, 60A.9852, and 60A.9853, subdivisions 3 to 5, provided the licensee submits a written statement certifying its compliance with HIPAA;

(3) a licensee affiliated with a depository institution that maintains an information security program in compliance with the interagency guidelines establishing standards for safeguarding customer information as set forth pursuant to United States Code, title 15, sections 6801 and 6805, shall be considered to meet the requirements of section 60A.9851 provided that the licensee produce, upon request, documentation satisfactory to the commission that independently validates the affiliated depository institution's adoption of an information security program that satisfies the interagency guidelines;

(4) an employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from sections 60A.9851 and 60A.9852 and need not develop its own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee; and

(5) an employee, agent, representative, or designee of a producer licensee, as defined under section 60K.31, subdivision 6, who is also a licensee, is exempt from sections 60A.985 to 60A.9857.

Subd. 2. **Exemption lapse; compliance.** In the event that a licensee ceases to qualify for an exception, such licensee shall have 180 days to comply with this act.

Sec. 8. **[60A.9857] PENALTIES.**

In the case of a violation of sections 60A.985 to 60A.9856, a licensee may be penalized in accordance with section 60A.052.

Sec. 9. **REPEALER.**

Minnesota Statutes 2020, sections 60A.98; 60A.981; and 60A.982, are repealed.

Sec. 10. **EFFECTIVE DATE.**

Sections 1 to 9 are effective August 1, 2021. Licensees have one year from the effective date to implement Minnesota Statutes, section 60A.9851, subdivisions 1 to 5 and 7 to 9, and two years from the effective date of this act to implement Minnesota Statutes, section 60A.9851, subdivision 6.

60A.98 DEFINITIONS.

Subdivision 1. **Scope.** For purposes of sections 60A.98 and 60A.981, the terms defined in this section have the meanings given them.

Subd. 2. **Customer.** "Customer" means a consumer who has a continuing relationship with a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family, or household purposes.

Subd. 3. **Customer information.** "Customer information" means nonpublic personal information about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the licensee.

Subd. 4. **Customer information systems.** "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

Subd. 5. **Licensee.** "Licensee" means all licensed insurers, producers, and other persons licensed or required to be licensed, authorized or required to be authorized, or registered or required to be registered pursuant to the insurance laws of this state, except that "licensee" does not include a purchasing group or an ineligible insurer in regard to the surplus line insurance conducted pursuant to sections 60A.195 to 60A.209. "Licensee" does not include producers until January 1, 2007.

Subd. 6. **Nonpublic financial information.** "Nonpublic financial information" means:

(1) personally identifiable financial information; and

(2) any list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived using any personally identifiable financial information that is not publicly available.

Subd. 7. **Nonpublic personal health information.** "Nonpublic personal health information" means health information:

(1) that identifies an individual who is the subject of the information; or

(2) with respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

Subd. 8. **Nonpublic personal information.** "Nonpublic personal information" means nonpublic financial information and nonpublic personal health information.

Subd. 9. **Personally identifiable financial information.** "Personally identifiable financial information" means any information:

(1) a consumer provides to a licensee to obtain an insurance product or service from the licensee;

(2) about a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(3) the licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

Subd. 10. **Service provider.** "Service provider" means a person that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the licensee.

60A.981 INFORMATION SECURITY PROGRAM.

Subdivision 1. **General requirements.** Each licensee shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information. The administrative, technical, and physical safeguards included in the information security program must be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Subd. 2. **Objectives.** A licensee's information security program must be designed to:

(1) ensure the security and confidentiality of customer information;

(2) protect against any anticipated threats or hazards to the security or integrity of the information; and

(3) protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Subd. 3. **Examples of methods of development and implementation.** The following actions and procedures are examples of methods of implementation of the requirements of subdivisions 1 and 2. These examples are nonexclusive illustrations of actions and procedures that licensees may follow to implement subdivisions 1 and 2:

(1) the licensee:

(i) identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

(ii) assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(iii) assesses the sufficiency of policies, procedures, customer information systems, and other safeguards in place to control risks;

(2) the licensee:

(i) designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

(ii) trains staff, as appropriate, to implement the licensee's information security program; and

(iii) regularly tests or otherwise regularly monitors the key controls, systems, and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment;

(3) the licensee:

(i) exercises appropriate due diligence in selecting its service providers; and

(ii) requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations; and

(4) the licensee monitors, evaluates, and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

60A.982 UNFAIR TRADE PRACTICES.

A violation of sections 60A.98 and 60A.981 is considered to be a violation of sections 72A.17 to 72A.32.