Bill Summary

H.F. 1913

As introduced

Subject	Insurance data security
Authors	Elkins
Analyst	Nathan Hopkins
Date	March 15, 2021

Overview

This bill requires insurance companies to establish an information security program to protect consumers' nonpublic data and report certain cybersecurity events. The bill provides for classification of the data received by the commissioner or commerce, establishes exceptions to the requirements, and provides for penalties if a licensee fails to comply with the new requirements.

Summary

Section	Description
1	**Definitions.** Defines terms including "cybersecurity event," "multifactor authentication," "nonpublic information," and "third-party service provider" as used in the new sections of law.
2	**Information security program.** **Subd. 1. Implementation of an information security program.** Requires licensees to develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment. **Subd. 2. Objectives of an information security program.** Requires an information security program to protect the security and confidentiality of nonpublic information and the information system; protect against threats or hazards to nonpublic information or the information system; protect against unauthorized access to, or use of, nonpublic information; and define and reevaluate a schedule from retention of nonpublic information. **Subd. 3. Risk assessment.** Requires licensees to identify a person responsible for the information security program; identify reasonably foreseeable threats; assess the likelihood of, and damage from, those threats; asses the sufficiency of policies, procedures, information systems, and other safeguards; and implement information safeguards to manage identified threats.

Section	Description

Subd. 4. Risk management. Directs licensees to design systems to mitigate identified risks, implement appropriate security measures, include cybersecurity risks in the licensee's enterprise risk management process, stay informed about possible threats, and provide personnel with cybersecurity awareness training.

Subd. 5. Oversight by board of directors. Directs a licensee's board of directors to require development and implementation of an information security program and require a report on that program.

Subd. 6. Oversight of third-party service provider arrangements. Requires licensees to exercise due diligence in selecting third-party service providers and directs licensees to require those third-party service providers to implement appropriate safeguards to protect information systems and nonpublic information.

Subd. 7. Program adjustments. Directs licensees to monitor and adjust the information security program consistent with new information or changes in technology.

Subd. 8. Incident response plan. Requires licensees to include an incident response plan as part of their information security programs and establishes minimum requirements for those plans.

Subd. 9. Annual certification to commissioner. Requires insurers domiciled in Minnesota to annually certify in writing that they are in compliance with this section, maintain records for five years, permit inspection of those records, document areas that require improvement, and permit inspection of that documentation.

3 **Investigation of a cybersecurity event.**

Requires a licensee to perform a prompt investigation after learning that a cybersecurity event may have occurred. The investigation must determine if an event took place and, if so, identify the nature and scope of the event and whether any nonpublic data was involved. Further requires a licensee to either perform an investigation or confirm that one has occurred if a cybersecurity event may have occurred in a system maintained by a third-party service provider. Requires the licensee to maintain records for five years and produce records on demand of the commissioner.

4 **Notification of a cybersecurity event.**

Subd. 1. Notification to the commissioner. Requires a licensee to notify the commissioner of commerce or the commissioner of health, as applicable, when a cybersecurity event occurred that involved a reasonable likelihood of material harm to a consumer or the normal operations of a licensee; or the licensee

Section	Description

reasonably believes that the nonpublic information involved belongs to 250 or more consumers living in Minnesota and either notice is required under other provisions or the event has a reasonable likelihood of material harm to a consumer or the normal operations of a licensee.

Subd. 2. Information; notification. The licensee providing notification must do so in electronic form and has a duty to update the information submitted. As applicable, notification should include information in 13 different categories including the date of the event, how the event was discovered, whether any data was recovered, and the results of any internal review.

Subd. 3. Notification to consumers. Requires a licensee to provide notice—in the manner prescribed under the subdivision—to a consumer if, as a result of a cybersecurity event, the consumer's nonpublic information was compromised in a way that poses a risk of material harm.

Subd. 4. Notice regarding cybersecurity events of third-party service providers. Requires a licensee to treat a cybersecurity event in a system maintained by a third-party service provider as it would treat an event under subdivision 1. Permits licensees to contract with third-party service providers regarding the duty comply with this subdivision.

Subd. 5. Notice regarding cybersecurity events of reinsurers to insurers. Requires a reinsurer to send notice of a cybersecurity event to the commissioner and to the ceding insurer. Directs the ceding insurer to send any relevant notification to the customer.

Subd. 6. Notice regarding cybersecurity events of insurers to producers of record. Requires insurers to notify the producers of record of all affected consumers following a cybersecurity event.

5 **Power of commissioner.**

Grants the commissioner of commerce or commissioner of health, as applicable, power to investigate a licensee to determine if the licensee engaged in conduct that violates the new law, and take appropriate enforcement action.

6 **Confidentiality.**

Subd. 1. Licensee information. Classifies data in the possession of the commissioner provided pursuant to the new law as confidential, protected nonpublic, or both, but permits the commissioner to use the data in a regulatory or legal action.

Subd. 2. Certain testimony prohibited. Provides that the commissioner and any other person who received the documents while acting under the authority of

Section	Description

the commissioner shall not be required to testify in any civil action concerning confidential documents or information.

Subd. 3. Information sharing. Permits the commissioner to receive and share certain documents and information with other entities including state, federal, and international regulatory agencies and the national Association of Insurance Commissioners.

Subd. 4. No waiver of privilege or confidentiality. Provides that sharing documents or information pursuant to subdivision 3 does not waive any applicable privilege or claim of confidentiality.

Subd. 5. Certain actions public. Permits the commissioner to release final, adjudicated actions that are open to the public pursuant to chapter 13.

Subd. 6. Classification, protection, and use of information by others. Provides that documents and other information in the possession or control of the national Association of Insurance Companies is classified as confidential, protected nonpublic, and privileged.

7 **Exceptions.**

Establishes exceptions for a licensee with fewer than 25 employees, licensees subject to other data privacy laws, licensees covered by the information security program of another licensee, and employees of a producer licensee.

8 **Penalties.**

Provides that violations of the new sections of law may be penalized in accordance with existing law, as described in section 60A.052, which includes suspension or revocation.

9 **Repealer.**

Repeals the current statutes requiring establishment of an information security program.

10 **Effective date.**

All sections are effective August 1, 2021. Licensees are given until August 1, 2022, to implement section 2 of the bill, except that licensees have two years to implement subdivision 6 of that section regarding third-party service providers.