SENATE BILL No. 240

DIGEST OF INTRODUCED BILL

Citations Affected: IC 27-2-27.

Synopsis: Cybersecurity requirements for insurers. Requires an insurer to: (1) develop, maintain, and update an information security program for the purpose of protecting consumers' nonpublic information; (2) conduct a risk assessment of its information systems to aid in the development of an information security program; (3) notify the insurance commissioner if a cybersecurity event affecting the nonpublic information of 250 or more consumers occurs; and (4) develop an incident response plan to respond to cybersecurity events.

Effective: July 1, 2020.

Brown L

January 9, 2020, read first time and referred to Committee on Insurance and Financial Institutions.

Introduced

Second Regular Session of the 121st General Assembly (2020)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type.~~

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.

Conflict reconciliation: Text in a statute in *this style type* or ~~*this style type*~~ reconciles conflicts between statutes enacted by the 2019 Regular Session of the General Assembly.

SENATE BILL No. 240

A BILL FOR AN ACT to amend the Indiana Code concerning insurance.

Be it enacted by the General Assembly of the State of Indiana:

SECTION 1. IC 27-2-27 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2020]:

Chapter 27. Insurance Data Security

Sec. 1. As used in this chapter, "authorized individual" means an individual:

(1) known to and screened by an insurer; and

(2) determined to be necessary and appropriate to have access to the nonpublic information held by the insurer and its information systems.

Sec. 2. As used in this chapter, "commissioner" means the insurance commissioner appointed under IC 27-1-1-2.

Sec. 3. As used in this chapter, "consumer" means a resident of Indiana whose nonpublic information is in an insurer's possession, custody, or control.

Sec. 4. As used in this chapter, "cybersecurity event" means an event resulting in unauthorized access to or a disruption or misuse

of an information system or nonpublic information stored on the information system. However, the term does not include the following:

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

(2) An event in which an insurer has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

Sec. 5. As used in this chapter, "department" means the department of insurance created by IC 27-1-1-1.

Sec. 6. As used in this chapter, "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.

Sec. 7. As used in this chapter, "information security program" means the administrative, technical, and physical safeguards that an insurer uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.

Sec. 8. As used in this chapter, "information system" means the following:

(1) A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of nonpublic information.

(2) Any specialized system, such as industrial or process control systems, telephone switching systems, private exchange systems, and environmental control systems.

Sec. 9. As used in this chapter, "insurer" means a company, firm, partnership, association, order, society, or system making any kind or kinds of insurance that employs twenty-five (25) or more employees.

Sec. 10. As used in this chapter, "multi-factor authentication" means authentication through verification of at least two (2) 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.

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

Sec. 11. As used in this chapter, "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; 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 consumer and relates to:

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

(B) the provision of health care to the consumer; or

(C) payment for the provision of health care provided to the consumer.

Sec. 12. As used in this chapter, "publicly available information" means any information that an insurer has a reasonable basis to believe is lawfully made available to the general public from:

(1) federal, state, or local government records;

(2) widely distributed media; or

(3) disclosures to the general public that are required to be made by federal, state, or local law.

Sec. 13. As used in this chapter, "risk assessment" means the assessment an insurer is required to conduct under section 16 of this chapter.

Sec. 14. As used in this chapter, "third party service provider" means a person that contracts with an insurer to maintain, process, store, or otherwise is permitted access to nonpublic information through its provision of services to the insurer.

Sec. 15. (a) An insurer shall develop, implement, and maintain a comprehensive, written information security program that:

(1) is based on the risk assessment required under section 16 of this chapter; and

(2) contains administrative, technical, and physical safeguards for the protection of nonpublic information and the insurer's information systems.

(b) An information security program must accomplish the following:

(1) Protect the security and confidentiality of nonpublic information and information systems.

(2) Protect against any threats or hazards to the security or integrity of nonpublic information and information systems.

(3) Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to a consumer.

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

Sec. 16. An insurer shall conduct a risk assessment of its information systems and treatment of nonpublic information by doing the following:

(1) Designating one (1) or more employees, an affiliate, or a third party service provider to assume responsibility for the insurer's information security program.

(2) Identifying reasonably foreseeable internal or external threats that could result in a cybersecurity event, including threats to information systems and nonpublic information held or accessed by third party service providers.

(3) Assessing the likelihood and potential damage of the threats identified in subdivision (2), taking into consideration the sensitivity of the nonpublic information.

(4) Assessing the sufficiency of the policies, procedures, information systems, and other safeguards currently in place to manage the threats identified in subdivision (2), including an assessment of threats in each relevant area of the insurer's operations, including the following:

(A) Employee training and management.

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

(C) Procedures for detecting, preventing, and responding to cybersecurity events or other systems failures.

(5) Implementing information safeguards to manage the threats identified in subdivision (2), and assessing the effectiveness of the safeguards' key controls, systems, and procedures at least one (1) time each year.

Sec. 17. Based on the results of the risk assessment, an insurer shall do the following:

(1) Design its information security program to mitigate the identified risks, commensurate with:

(A) the insurer's size and complexity;

(B) the nature and scope of the insurer's activities; and

(C) the sensitivity of the nonpublic information in the insurer's control.

(2) Determine and implement appropriate security measures, which may include the following:

(A) Placing access controls on information systems, including controls to authenticate and permit only authorized individuals to have access to nonpublic information.

(B) Identifying and managing the data, personnel, devices, systems, and facilities that enable the insurer to achieve business purposes in accordance with their relative importance to business objectives and risk strategy.

(C) Restricting physical access to nonpublic information to authorized individuals only.

(D) Protecting 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.

(E) Adopting secure development practices for in-house developed applications used by the insurer.

(F) Modifying information systems in accordance with the insurer's information security program.

(G) Using effective controls, which may include multi-factor authentication procedures for any person accessing nonpublic information.

(H) Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

(I) Including audit trails within the information security program designed to detect and respond to a cybersecurity event and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the insurer.

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

(K) Developing, implementing, and maintaining procedures for the secure disposal of nonpublic information in any format.

(3) Include cybersecurity risks in the insurer's enterprise risk management process.

(4) Stay informed regarding emerging threats or

vulnerabilities.

(5) Use reasonable security measures when sharing information, relative to the character of the sharing and the type of information shared.

(6) Provide personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified in the risk assessment.

Sec. 18. (a) If the insurer has a board of directors, the board of directors shall require the insurer's executive management or its delegates to:

(1) develop, implement, and maintain the insurer's information security program; and

(2) report in writing, at least annually, the following information:

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

(B) Material matters related to the information security program, including risk assessment, risk management, control decisions, third party service provider arrangements, cybersecurity events, and recommendations for changes in the information security program.

(b) If the insurer's executive management delegates any of its responsibilities under this section, it shall:

(1) oversee the development, implementation, and maintenance of the insurer's information security program prepared by the delegate; and

(2) receive a report from the delegate complying with the requirements of the report to the board of directors required by subsection (a)(2).

Sec. 19. (a) As part of its information security program, an insurer shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event.

(b) An incident response plan must include the following:

(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.

(7) The evaluation and revision as necessary of the incident response plan.

Sec. 20. (a) If an insurer learns that a cybersecurity event has or may have occurred, the insurer or its delegate shall conduct a prompt investigation. During the investigation, the insurer or its delegate shall determine the following information:

(1) Whether a cybersecurity event has occurred.

(2) The nature and scope of the cybersecurity event.

(3) Any nonpublic information that may have been involved in the cybersecurity event.

(b) An insurer shall maintain records concerning all cybersecurity events for at least five (5) years from the date of the cybersecurity event. An insurer shall produce these records upon demand of the commissioner.

(c) An insurer shall notify the commissioner not later than three (3) business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of the insurer has occurred when the insurer reasonably believes that the nonpublic information of at least two hundred fifty (250) consumers was affected by the cybersecurity event and that the cybersecurity event is either of the following:

(1) A cybersecurity event impacting the insurer of which notice is required to be provided by any other state, federal, or local law.

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

(A) a consumer; or

(B) any material part of the normal operations of the insurer.

Sec. 21. This chapter does not create a private right of action against any person.