ENGROSSED SENATE
BILL NO. 1919

By: Stanislawski of the Senate

and

Sims of the House

[insurance - Insurance Data Security Act - comprehensive information security program - codification - effective date]

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

SECTION 1. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 670 of Title 36, unless there is created a duplication in numbering, reads as follows:

This act shall be known and may be cited as the "Insurance Data Security Act".

SECTION 2. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 671 of Title 36, unless there is created a duplication in numbering, reads as follows:

As used in this act:

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 its information systems;

2. “Commissioner” means the Insurance Commissioner of this state;

3. “Consumer” means an individual including but not limited to applicants, policyholders, insureds, beneficiaries, claimants and certificate holders who are a resident of this state and whose nonpublic information is in the possession, custody or control of a licensee;

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 cybersecurity event shall 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 in 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;

5. “Department” means the Insurance Department;

6. “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;

7. “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;

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 such as industrial and process controls systems, telephone switching and private branch exchange systems and environmental control systems;

9. "Licensee" means any person licensed, authorized to operate or registered, or required to be licensed, authorized or registered pursuant to Title 36 of the Oklahoma Statutes; provided, however, that it shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a person 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 (2) of the following types of authentication factors:

a. knowledge factor, such as a password,

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

c. inherence factor, such as a biometric characteristic;

11. "Non-public information" means electronic information that is not publicly available and is:

a. business related information of a licensee, of which the tampering with or unauthorized disclosure, access or use of would cause a material adverse impact to the business, operations or security of the licensee,

b. any information concerning a consumer that, because of name, number, personal mark or other identifier, can be used to identify him or her, in combination with any one or more of the following data elements:

(1) Social Security number,

(2) driver license number or nondriver identification card number,

(3) financial account number, 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, and

c. 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:

(1) the past, present or future physical, mental or behavioral health or condition of any consumer or a member of the family of the consumer,

(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 but not limited to any nongovernmental partnership, corporation, branch, agency or association;

13. "Publicly available information" means any information that a licensee has 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:

a. that the information is of the type that is available to the general public, and

b. 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; and

14. "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.

SECTION 3. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 672 of Title 36, unless there is created a duplication in numbering, reads as follows:

A. Each licensee in this state shall develop, implement and maintain a comprehensive written information security program based on the risk assessment of the licensee provided for in this act and that contains administrative, technical and physical safeguards for the protection of nonpublic information and the information system of the licensee. The program shall be commensurate with the size and complexity of the licensee, the nature and scope of the activities of the licensee including its use of third-party service providers and the sensitivity of the nonpublic information used by the licensee or in the possession, custody or control of the licensee.

B. An information security program of a licensee 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.

C. The licensee shall:

1. Designate one or more employees, an affiliate or an outside vendor designated 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 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 these threats, 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 operations of the licensee including:

a. employee training and management,

b. information systems including network and software design, as well as information classification, governance, processing, storage, transmission and disposal, and

c. 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 key controls, systems and procedures of the safeguards.

D. Based on the results of the 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 activities of the licensee including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the possession, custody or control of the licensee;

2. Determine which security measures listed below are appropriate and implement such security measures:

a. 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,

b. 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 risk strategy of the organization,

c. restrict physical access to nonpublic information, to authorized individuals only,

d. 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,

e. adopt secure development practices for in-house developed applications utilized by the licensee,

f. modify the information system in accordance with the information security program of the licensee,

g. utilize effective controls, which may include multi-factor authentication procedures for accessing nonpublic information,

h. regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems,

i. 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,

j. implement measures to protect against destruction, loss or damage of nonpublic information due to environmental hazards such as fire and water damage or other catastrophic events or technological failures, and

k. develop, implement and maintain procedures for the secure disposal of nonpublic information in any format;

3. Include cybersecurity risks in the enterprise risk management process of the licensee;

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.

E. If the licensee has a board of directors, the board or an appropriate committee of the board shall, within one year of the effective date of this act:

1. Require the executive management of the licensee of its delegates to develop, implement and maintain the information security program of the licensee;

2. Require the executive management of the licensee or its delegates to report in writing, annually, the following information:

a. the overall status of the information security program and the compliance of the licensee with this act, and

b. 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 responses of the management to those events or violations and recommendations for changes in the information security program; and

3. If executive management delegates any of its responsibilities, it shall oversee the development, implementation and maintenance of the information security program of the licensee prepared by the delegate or delegates and shall receive a report from the delegate or delegates complying with the requirements of the report to the board.

F. A licensee shall, within one year of the effective date of this act, exercise due diligence in selecting its third-party service provider and shall require the 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.

G. 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 changing business arrangements of the licensee, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

H. 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 information systems of the licensee or the continuing functionality of any aspect of the business or operations of the licensee.

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.

I. Annually, each insurer domiciled in this state shall submit to the Insurance Commissioner a written statement by February 15, certifying that the insurer complies with the requirements set forth in Section 663 of Title 36 of the Oklahoma Statutes. Each insurer shall maintain, for examination by the Insurance Department, all records, schedules and data supporting this certificate for a period of five (5) 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 such areas, systems or processes. The documentation shall be available for inspection by the Commissioner upon request.

SECTION 4. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 673 of Title 36, unless there is created a duplication in numbering, reads as follows:

A. 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.

B. During the investigation, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall, at a minimum determine as much of the following information as possible:

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; and

4. 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 possession, custody or control of the licensee.

C. The licensee shall maintain records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event and shall produce those records upon request by the Insurance Commissioner.

SECTION 5. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 674 of Title 36, unless there is created a duplication in numbering, reads as follows:

A. Every licensee shall notify the Insurance Commissioner without unreasonable delay, but not later than three (3) business

days, from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred when either of the following criteria has been met:

1. This state is the state of domicile of the licensee, in the case of an insurer, or this state is the home state of the licensee, in the case of a producer, as those terms are defined in the Oklahoma Producer Licensing Act, Sections 1435.1 through 1435.41 of Title 36 of the Oklahoma Statutes, and the cybersecurity event has a reasonable likelihood of substantially harming a material part of the normal operations of the licensee or any consumer residing in this state; or

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

a. 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

b. a cybersecurity event that has a reasonable likelihood of materially harming:

(1) any consumer residing in this state, or

(2) any material part of the normal operation or operations of the licensee.

B. The licensee making the notification required in subsection A of this section shall provide as much of the following information as possible, in a form to be prescribed by the Commissioner:

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, but not limited to, types of medical information, financial information or 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 privacy policy of the licensee 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 both familiar with the cybersecurity event and authorized to act for the licensee.

The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner regarding material changes to previously provided information relating to the cybersecurity event.

C. A licensee shall comply with the procedures of the Security Breach Notification Act, Section 161 et seq. of Title 24 of the Oklahoma Statutes, to notify affected consumers and provide a copy of the notice sent to consumers under that statute to the Commissioner, when a licensee is required to notify the Commissioner under subsection A of this section.

D. 1. 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 as it would under subsection A of this section unless the third-party service provider provides the notice required under subsection A of this section to the Commissioner and the licensee.

2. The computation of deadlines of the licensee 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.

3. Nothing in this subsection 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 or notice requirements imposed under this act.

E. 1. 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 (3) business days of making the determination 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 the Security Breach

Notification Act, Section 161 et seq. of Title 24 of the Oklahoma Statutes and any other notification requirements relating to a cybersecurity event imposed under this section.

2. 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 (3) 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 Security Breach Notification Act, Section 161 et seq. of Title 24 of the Oklahoma Statutes and any other notification requirements relating to a cybersecurity event imposed under this section.

F. 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 for which a consumer accessed the services of the insurer through an independent insurance producer, and for which consumer notice is required by this act or the Security Breach Notification Act, Section 161 et seq. of Title 24 of the Oklahoma Statutes, 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 this obligation for any producers who are not authorized by law or contract to sell, solicit or negotiate on behalf of the insurer, and in those instances in which the insurer does not have the current producer of record information for an individual consumer. 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 or any other law of this state.

SECTION 6. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 675 of Title 36, unless there is created a duplication in numbering, reads as follows:

A. The Insurance Commissioner shall have power to examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of the provisions of this act. This power is in addition to the powers which the Commissioner has under Section 309.1 through 309.6 of Title 36 of the Oklahoma Statutes. Any investigation or examination shall be conducted pursuant to Section 309.1 through 309.6 of Title 36 of the Oklahoma Statutes.

B. Whenever the Commissioner has reason to believe that a licensee has been or is engaged in conduct in this state that

violates any provision of this act, the Commissioner may take action that is necessary or appropriate to enforce the provisions.

SECTION 7. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 676 of Title 36, unless there is created a duplication in numbering, reads as follows:

A. Any documents, materials or other information in the control or possession of the Insurance Department that are furnished by a licensee or an employee or agent thereof acting on behalf of a licensee pursuant to the provisions of Section 4 and Section 5 of this act or that are obtained by the Insurance Commissioner in an investigation or examination pursuant to Section 6 of this act shall be confidential by law and privileged, shall not be subject to the Oklahoma Open Records Act, 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. The Commissioner shall not otherwise make the documents, materials or other information public without the prior written consent of the licensee.

B. 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 subsection A of this section.

C. In order to assist in the performance of the duties of the Commissioner under this act, the Commissioner:

1. May share documents, materials or other information including the confidential and privileged documents, materials or information subject to subsection A of this section, with other state, federal and international regulatory agencies, with the National Association of Insurance Commissioners and 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 subsection A of 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

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

D. 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 subsection C of this section.

E. Nothing in this act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to the Oklahoma Open Records Act to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

F. 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 act shall be confidential by law and privileged, shall not be subject to the Oklahoma Open Records Act, shall not be subject to subpoena, and

shall not be subject to discovery or admissible as evidence in any private civil action.

SECTION 8. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 677 of Title 36, unless there is created a duplication in numbering, reads as follows:

A. The Insurance Commissioner shall promulgate rules to implement the provisions of this section.

B. 1. The following exceptions shall apply to this act:

a. a licensee with fewer than twenty (20) employees including any independent contractor, is exempt from this act,

b. a licensee subject to the Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936, as amended, that has established and maintains an Information Security Program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 3 of this act; provided, that the licensee is compliant with and submits a written statement to the Commissioner certifying its compliance with, the same, and

c. an employee, agent, representative or designee of a licensee, who is also a licensee, is exempt from this act and shall not be required to develop their own

information security program to the extent that the employee, agent, representative or designee is covered by the information security program of the licensee.

2. If a licensee ceases to qualify for an exception, the licensee shall have one hundred eighty (180) days to comply with the provisions of this act.

C. In the case of a violation of this act, a licensee may be penalized in accordance with Sections 908 and 1435.26 of Title 36 of the Oklahoma Statutes, or any other provision providing for penalties that the licensee is subject to under the license or permit of the licensee. Nothing in this act shall be construed to impose any civil liability for any violation of this act or omission to act by the licensee or employees of the licensee.

D. The provisions of this act shall take precedence over any other state laws applicable to licensees for data security and the investigation of a cybersecurity event.

SECTION 9. This act shall become effective November 1, 2020.

Passed the Senate the 10th day of March, 2020.

_____
Presiding Officer of the Senate

Passed the House of Representatives the ____ day of _____, 2020.

_____
Presiding Officer of the House of Representatives