

1 **SENATE FLOOR VERSION**

2 February 26, 2020

3 COMMITTEE SUBSTITUTE  
4 FOR

5 SENATE BILL NO. 1919

By: Stanislawski of the Senate

and

Sims of the House

6  
7  
8  
9 [ insurance - Insurance Data Security Act -  
10 comprehensive information security program -  
11 codification - effective date ]  
12

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

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

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

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

22 As used in this act:

23 1. "Authorized individual" means an individual known to and  
24 screened by the licensee and determined to be necessary and

1 appropriate to have access to the nonpublic information held by the  
2 licensee and its information systems;

3 2. "Commissioner" means the Insurance Commissioner of this  
4 state;

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

10 4. "Cybersecurity event" means an event resulting in  
11 unauthorized access to, disruption or misuse of, an information  
12 system or nonpublic information stored on the information system.

13 The term cybersecurity event shall not include the unauthorized  
14 acquisition of encrypted nonpublic information if the encryption,  
15 process or key is not also acquired, released or used without  
16 authorization. Cybersecurity event does not include an event in  
17 which the licensee has determined that the nonpublic information  
18 accessed by an unauthorized person has not been used or released and  
19 has been returned or destroyed;

20 5. "Department" means the Insurance Department;

21 6. "Encrypted" means the transformation of data into a form  
22 which results in a low probability of assigning meaning without the  
23 use of a protective process or key;

24

1       7. "Information security program" means the administrative,  
2 technical and physical safeguards that a licensee uses to access,  
3 collect, distribute, process, protect, store, use, transmit, dispose  
4 of or otherwise handle nonpublic information;

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

12       9. "Licensee" means any person licensed, authorized to operate  
13 or registered, or required to be licensed, authorized or registered  
14 pursuant to Title 36 of the Oklahoma Statutes, provided, however,  
15 that it shall not include a purchasing group or a risk retention  
16 group chartered and licensed in a state other than this state or a  
17 person that is acting as an assuming insurer that is domiciled in  
18 another state or jurisdiction;

19       10. "Multi-factor authentication" means authentication through  
20 verification of at least two (2) of the following types of  
21 authentication factors:

- 22           a. knowledge factors, such as a password,
- 23           b. possession factors, such as a token or text message on  
24                a mobile phone, or

1 c. inherence factors, such as a biometric characteristic;

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

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

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

12 (1) Social Security number,

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

15 (3) financial account number, credit or debit card  
16 number,

17 (4) any security code, access code or password that  
18 would permit access to a consumer's financial  
19 account, or

20 (5) biometric records, and

21 c. any information or data, except age or gender, in any  
22 form or medium created by or derived from a health  
23 care provider or a consumer that can be used to  
24 identify a particular consumer and that relates to:

- 1 (1) the past, present or future physical, mental or  
2 behavioral health or condition of any consumer  
3 or a member of the family of the consumer,  
4 (2) the provision of health care to any consumer, or  
5 (3) payment for the provision of health care to any  
6 consumer;

7 12. "Person" means any individual or any nongovernmental  
8 entity including but not limited to any nongovernmental  
9 partnership, corporation, branch, agency or association;

10 13. "Publicly available information" means any information that  
11 a licensee has reasonable basis to believe is lawfully made  
12 available to the general public from federal, state or local  
13 government records, widely distributed media or disclosures to the  
14 general public that are required to be made by federal, state or  
15 local law.

16 For the purposes of this definition, a licensee has a reasonable  
17 basis to believe that information is lawfully made available to the  
18 general public if the licensee has taken steps to determine:

- 19 a. that the information is of the type that is available  
20 to the general public, and  
21 b. whether a consumer can direct that the information not  
22 be made available to the general public and, if so,  
23 that such consumer has not done so; and  
24

1 14. "Third-party service provider" means a person, not  
2 otherwise defined as a licensee, that contracts with a licensee to  
3 maintain, process, store or otherwise is permitted access to  
4 nonpublic information through its provision of services to the  
5 licensee.

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

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

19 B. An information security program of a licensee shall be  
20 designed to:

21 1. Protect the security and confidentiality of nonpublic  
22 information and the security of the information system;

23 2. Protect against any threats or hazards to the security or  
24 integrity of nonpublic information and the information system;

1 3. Protect against unauthorized access to or use of nonpublic  
2 information, and minimize the likelihood of harm to any consumer;  
3 and

4 4. Define and periodically reevaluate a schedule for retention  
5 of nonpublic information and a mechanism for its destruction when no  
6 longer needed.

7 C. The licensee shall:

8 1. Designate one or more employees, an affiliate or an outside  
9 vendor designated to act on behalf of the licensee who is  
10 responsible for the information security program;

11 2. Identify reasonably foreseeable internal or external threats  
12 that could result in unauthorized access, transmission, disclosure,  
13 misuse, alteration or destruction of nonpublic information including  
14 the security of information systems and nonpublic information that  
15 are accessible to, or held by, third-party service providers;

16 3. Assess the likelihood and potential damage of these threats,  
17 taking into consideration the sensitivity of the nonpublic  
18 information;

19 4. Assess the sufficiency of policies, procedures, information  
20 systems and other safeguards in place to manage these threats,  
21 including consideration of threats in each relevant area of the  
22 operations of the licensee including:

23 a. employee training and management,  
24

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

5           c. detecting, preventing and responding to attacks,  
6           intrusions or other systems failures; and

7           5. Implement information safeguards to manage the threats  
8 identified in its ongoing assessment, and no less than annually,  
9 assess the effectiveness of the key controls, systems and procedures  
10 of the safeguards.

11          D. Based on the results of the risk assessment, the licensee  
12 shall:

13          1. Design its information security program to mitigate the  
14 identified risks, commensurate with the size and complexity of the  
15 licensee, the nature and scope of the activities of the licensee  
16 including its use of third-party service providers, and the  
17 sensitivity of the nonpublic information used by the licensee or in  
18 the possession, custody or control of the licensee;

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

21           a. place access controls on information systems  
22           including controls to authenticate and permit access  
23           only to authorized individuals to protect against the  
24           unauthorized acquisition of nonpublic information,

- 1           b. identify and manage the data, personnel, devices,  
2           systems and facilities that enable the organization to  
3           achieve business purposes in accordance with their  
4           relative importance to business objectives and the risk  
5           strategy of the organization,
- 6           c. restrict physical access to nonpublic information, to  
7           authorized individuals only,
- 8           d. protect by encryption or other appropriate means, all  
9           nonpublic information while being transmitted over an  
10          external network and all nonpublic information stored  
11          on a laptop computer or other portable computing or  
12          storage device or media,
- 13          e. adopt secure development practices for in-house  
14          developed applications utilized by the licensee,
- 15          f. modify the information system in accordance with the  
16          information security program of the licensee,
- 17          g. utilize effective controls, which may include multi-  
18          factor authentication procedures for accessing  
19          nonpublic information,
- 20          h. regularly test and monitor systems and procedures to  
21          detect actual and attempted attacks on, or intrusions  
22          into, information systems,
- 23          i. include audit trails within the information security  
24          program designed to detect and respond to

1 cybersecurity events and designed to reconstruct  
2 material financial transactions sufficient to support  
3 normal operations and obligations of the licensee,  
4 j. implement measures to protect against destruction,  
5 loss or damage of nonpublic information due to  
6 environmental hazards such as fire and water damage or  
7 other catastrophic events or technological failures,  
8 and

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

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

13 4. Stay informed regarding emerging threats or vulnerabilities  
14 and utilize reasonable security measures when sharing information  
15 relative to the character of the sharing and the type of information  
16 shared; and

17 5. Provide its personnel with cybersecurity awareness training  
18 that is updated as necessary, to reflect risks identified by the  
19 licensee in the risk assessment.

20 E. If the licensee has a board of directors, the board or an  
21 appropriate committee of the board shall, at a minimum:

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

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

- 3           a. the overall status of the information security program  
4           and the compliance of the licensee with this act, and  
5           b. material matters related to the information security  
6           program, addressing issues such as risk assessment,  
7           risk management and control decisions, third-party  
8           service provider arrangements, results of testing,  
9           cybersecurity events or violations and responses of  
10          the management to those events or violations and  
11          recommendations for changes in the information  
12          security program; and

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

19          F. A licensee shall exercise due diligence in selecting its  
20 third-party service provider and shall require the provider to  
21 implement appropriate administrative, technical and physical  
22 measures to protect and secure the information systems and nonpublic  
23 information that are accessible to, or held by, the third-party  
24 service provider.

1 G. The licensee shall monitor, evaluate and adjust, as  
2 appropriate, the information security program consistent with any  
3 relevant changes in technology, the sensitivity of its nonpublic  
4 information, internal or external threats to information and the  
5 changing business arrangements of the licensee, such as mergers and  
6 acquisitions, alliances and joint ventures, outsourcing arrangements  
7 and changes to information systems.

8 H. As part of its information security program, each licensee  
9 shall establish a written incident response plan designed to  
10 promptly respond to, and recover from, any cybersecurity event that  
11 compromises the confidentiality, integrity or availability of  
12 nonpublic information in its possession, the information systems of  
13 the licensee or the continuing functionality of any aspect of the  
14 business or operations of the licensee.

15 The incident response plan shall address the following areas:

- 16 1. The internal process for responding to a cybersecurity event;
- 17 2. The goals of the incident response plan;
- 18 3. The definition of clear roles, responsibilities and levels of  
19 decision-making authority;
- 20 4. External and internal communications and information sharing;
- 21 5. Identification of requirements for the remediation of any  
22 identified weaknesses in information systems and associated  
23 controls;

24

1       6. Documentation and reporting regarding cybersecurity events  
2 and related incident response activities; and

3       7. The evaluation and revision as necessary of the incident  
4 response plan following a cybersecurity event.

5       I. Annually, each insurer domiciled in this state shall submit  
6 to the Insurance Commissioner a written statement by February 15,  
7 certifying that the insurer complies with the requirements set forth  
8 in Section 663 of Title 36 of the Oklahoma Statutes. Each insurer  
9 shall maintain, for examination by the Insurance Department, all  
10 records, schedules and data supporting this certificate for a period  
11 of five (5) years. To the extent an insurer has identified areas,  
12 systems or processes that require material improvement, updating or  
13 redesign, the insurer shall document the identification and the  
14 remedial efforts planned and underway to address such areas, systems  
15 or processes. The documentation shall be available for inspection by  
16 the Commissioner upon request.

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

20       A. If the licensee learns that a cybersecurity event has or  
21 may have occurred the licensee, or an outside vendor or service  
22 provider designated to act on behalf of the licensee, shall conduct  
23 a prompt investigation.

24

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

- 5 1. Whether a cybersecurity event has occurred;
- 6 2. The nature and scope of the cybersecurity event;
- 7 3. Any nonpublic information that may have been involved in the  
8 cybersecurity event; and
- 9 4. Reasonable measures to restore the security of the  
10 information systems compromised in the cybersecurity event in order  
11 to prevent further unauthorized acquisition, release or use of  
12 nonpublic information in the possession, custody or control of the  
13 licensee.

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

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

21 A. Every licensee shall notify the Insurance Commissioner  
22 without unreasonable delay, but not later than three (3) business  
23 days, from a determination that a cybersecurity event involving  
24

1 nonpublic information that is in the possession of a licensee has  
2 occurred when either of the following criteria has been met:

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

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

14 a. a cybersecurity event impacting the licensee of which  
15 notice is required to be provided to any government  
16 body, self-regulatory agency or any other supervisory  
17 body pursuant to any state or federal law, or

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

20 (1) any consumer residing in this state, or

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

23

24

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

- 4 1. Date of the cybersecurity event;
- 5 2. Description of how the information was exposed, lost, stolen  
6 or breached including the specific roles and responsibilities of  
7 third-party service providers, if any;
- 8 3. How the cybersecurity event was discovered;
- 9 4. Whether any lost, stolen or breached information has been  
10 recovered and, if so, how this was done;
- 11 5. The identity of the source of the cybersecurity event;
- 12 6. Whether the licensee has filed a police report or has  
13 notified any regulatory, government or law enforcement agencies and,  
14 if so, when such notification was provided;
- 15 7. Description of the specific types of information acquired  
16 without authorization. Specific types of information means  
17 particular data elements including, but not limited to, types of  
18 medical information, financial information or information allowing  
19 identification of the consumer;
- 20 8. The period during which the information system was  
21 compromised by the cybersecurity event;
- 22 9. The number of total consumers in this state affected by the  
23 cybersecurity event. The licensee shall provide the best estimate  
24 in the initial report to the Commissioner and update this estimate

1 with each subsequent report to the Commissioner pursuant to this  
2 section;

3 10. The results of any internal review identifying a lapse in  
4 either automated controls or internal procedures, or confirming that  
5 all automated controls or internal procedures were followed;

6 11. Description of efforts being undertaken to remediate the  
7 situation which permitted the cybersecurity event to occur;

8 12. A copy of the privacy policy of the licensee and a  
9 statement outlining the steps the licensee will take to investigate  
10 and notify consumers affected by the cybersecurity event; and

11 13. Name of a contact person who is both familiar with the  
12 cybersecurity event and authorized to act for the licensee.

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

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

23 D. 1. In the case of a cybersecurity event in a system  
24 maintained by a third-party service provider, of which the licensee

1 has become aware, the licensee shall treat the event as it would  
2 under subsection A of this section unless the third-party service  
3 provider provides the notice required under subsection A of this  
4 section to the Commissioner and the licensee.

5 2. The computation of deadlines of the licensee shall begin on  
6 the day after the third-party service provider notifies the licensee  
7 of the cybersecurity event or the licensee otherwise has actual  
8 knowledge of the cybersecurity event, whichever is sooner.

9 3. Nothing in this subsection shall prevent or abrogate an  
10 agreement between a licensee and another licensee, a third-party  
11 service provider or any other party to fulfill any of the  
12 investigation requirements imposed or notice requirements imposed  
13 under this act.

14 E. 1. In the case of a cybersecurity event involving nonpublic  
15 information that is used by the licensee that is acting as an  
16 assuming insurer, or in the possession, custody or control of a  
17 licensee, that is acting as an assuming insurer and that does not  
18 have a direct contractual relationship with the affected consumers,  
19 the assuming insurer shall notify its affected ceding insurers and  
20 the Commissioner of its state of domicile within three (3) business  
21 days of making the determination that a cybersecurity event has  
22 occurred. The ceding insurers that have a direct contractual  
23 relationship with affected consumers shall fulfill the consumer  
24 notification requirements imposed under the Security Breach

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

4       2. In the case of a cybersecurity event involving nonpublic  
5 information that is in the possession, custody or control of a  
6 third-party service provider of a licensee that is an assuming  
7 insurer, the assuming insurer shall notify its affected ceding  
8 insurers and the Commissioner of its state of domicile within three  
9 (3) business days of receiving notice from its third-party service  
10 provider that a cybersecurity event has occurred. The ceding  
11 insurers that have a direct contractual relationship with affected  
12 consumers shall fulfill the consumer notification requirements  
13 imposed under Security Breach Notification Act, Section 161 et seq.  
14 of Title 24 of the Oklahoma Statutes and any other notification  
15 requirements relating to a cybersecurity event imposed under this  
16 section.

17       F. In the case of a cybersecurity event involving nonpublic  
18 information that is in the possession, custody or control of a  
19 licensee that is an insurer or its third-party service provider for  
20 which a consumer accessed the services of the insurer through an  
21 independent insurance producer, and for which consumer notice is  
22 required by this act or the Security Breach Notification Act,  
23 Section 161 et seq. of Title 24 of the Oklahoma Statutes, the  
24 insurer shall notify the producers of record of all affected

1 consumers of the cybersecurity event no later than the time at which  
2 notice is provided to the affected consumers.

3 The insurer is excused from this obligation for any producers  
4 who are not authorized by law or contract to sell, solicit or  
5 negotiate on behalf of the insurer, and in those instances in which  
6 the insurer does not have the current producer of record information  
7 for an individual consumer. Any licensee acting as an assuming  
8 insurer shall have no other notice obligations relating to a  
9 cybersecurity event or other data breach under this section or any  
10 other law of this state.

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

14 A. The Insurance Commissioner shall have power to examine and  
15 investigate the affairs of any licensee to determine whether the  
16 licensee has been or is engaged in any conduct in violation of the  
17 provisions of this act. This power is in addition to the powers  
18 which the Commissioner has under Section 309.1 through 309.6 of  
19 Title 36 of the Oklahoma Statutes. Any investigation or examination  
20 shall be conducted pursuant to Section 309.1 through 309.6 of Title  
21 36 of the Oklahoma Statutes.

22 B. Whenever the Commissioner has reason to believe that a  
23 licensee has been or is engaged in conduct in this state that  
24

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

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

6 A. Any documents, materials or other information in the control  
7 or possession of the Insurance Department that are furnished by a  
8 licensee or an employee or agent thereof acting on behalf of a  
9 licensee pursuant to the provisions of Section 4 and Section 5 of  
10 this act or that are obtained by the Insurance Commissioner in an  
11 investigation or examination pursuant to Section 6 of this act shall  
12 be confidential by law and privileged, shall not be subject to the  
13 Oklahoma Open Records Act, shall not be subject to subpoena, and  
14 shall not be subject to discovery or admissible in evidence in any  
15 private civil action. However, the Commissioner is authorized to  
16 use the documents, materials or other information in the furtherance  
17 of any regulatory or legal action brought as a part of the  
18 Commissioner's duties. The Commissioner shall not otherwise make  
19 the documents, materials or other information public without the  
20 prior written consent of the licensee.

21 B. Neither the Commissioner nor any person who received  
22 documents, materials or other information while acting under the  
23 authority of the Commissioner shall be permitted or required to  
24 testify in any private civil action concerning any confidential

1 documents, materials or information subject to subsection A of this  
2 section.

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

5 1. May share documents, materials or other information,  
6 including the confidential and privileged documents, materials or  
7 information subject to subsection A of this section, with other  
8 state, federal and international regulatory agencies, with the  
9 National Association of Insurance Commissioners and its affiliates  
10 or subsidiaries and with state, federal and international law  
11 enforcement authorities, provided that the recipient agrees in  
12 writing to maintain the confidentiality and privileged status of the  
13 document, material or other information;

14 2. May receive documents, materials or information, including  
15 otherwise confidential and privileged documents, materials or  
16 information, from the National Association of Insurance  
17 Commissioners, its affiliates or subsidiaries and from regulatory  
18 and law enforcement officials of other foreign or domestic  
19 jurisdictions, and shall maintain as confidential or privileged any  
20 document, material or information received with notice or the  
21 understanding that it is confidential or privileged under the laws  
22 of the jurisdiction that is the source of the document, material or  
23 information;

24

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

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

8           D. No waiver of any applicable privilege or claim of  
9 confidentiality in the documents, materials or information shall  
10 occur as a result of disclosure to the Commissioner under this  
11 section or as a result of sharing as authorized in subsection C of  
12 this section.

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

19           F. Documents, materials or other information in the possession  
20 or control of the National Association of Insurance Commissioners or  
21 a third-party consultant or vendor pursuant to this act shall be  
22 confidential by law and privileged, shall not be subject to the  
23 Oklahoma Open Records Act, shall not be subject to subpoena, and  
24

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

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

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

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

9 1. A licensee with fewer than ten (10) employees, including any  
10 independent contractors, is exempt from Section 3 of this act;

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

19 3. An employee, agent, representative or designee of a  
20 licensee, who is also a licensee, is exempt from Section 3 of this  
21 act and shall not be required to develop its own information  
22 security program to the extent that the employee, agent,  
23 representative or designee is covered by the information security  
24 program of the licensee.

1 C. In the event that a licensee ceases to qualify for an  
2 exception, the licensee shall have one hundred eighty (180) days to  
3 comply with the provisions of this act.

4 D. In the case of a violation of this act, a licensee may be  
5 penalized in accordance with Sections 908 and 1435.26 of Title 36 of  
6 the Oklahoma Statutes, or any other provision providing for  
7 penalties that the licensee is subject to under the license or  
8 permit of the licensee.

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

10 COMMITTEE REPORT BY: COMMITTEE ON APPROPRIATIONS  
11 February 26, 2020 - DO PASS AS AMENDED  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24