

1 ENGROSSED SENATE  
2 BILL NO. 543

By: Montgomery of the Senate

and

Sneed of the House

3  
4  
5  
6 An Act relating to insurance data security; creating  
7 the Insurance Data Security Act; providing short  
8 title; establishing act jurisdiction; construing  
9 provision; defining terms; requiring licensees to  
10 develop data security program with certain  
11 inclusions; establishing intent of security programs  
12 created pursuant to act; directing licensee to  
13 conduct risk assessment; directing licensee to take  
14 certain action following risk assessment result;  
15 requiring certain supervising boards to take certain  
16 actions to implement program; requiring licensee to  
17 contract with third-party service provider subject to  
18 certain conditions; requiring licensee to maintain  
19 updates and revisions to program; requiring licensee  
20 develop incident response plan; requiring certain  
21 reports be submitted to the Insurance Commissioner;  
22 requiring insurer to maintain certain records for  
23 specific time period; requiring investigation after  
24 certain cybersecurity event; establishing  
investigation process; requiring notification of  
certain event to the Commissioner; requiring  
compliance with certain state laws; providing for  
certain exemption; providing for the Commissioner to  
investigate certain licensees for certain violations;  
providing for confidentiality of certain information  
relating to cybersecurity event; allowing  
Commissioner to share certain data with national  
association; construing provision; providing for rule  
promulgation; providing certain exceptions to act;  
establishing penalties; amending 51 O.S. 2021,  
Section 24A.3, as last amended by Section 1, Chapter  
402, O.S.L. 2022 (51 O.S. Supp. 2022, Section 24A.3),  
which relates to the Oklahoma Open Records Act;  
modifying definition; updating statutory language;  
providing for codification; and providing an  
effective date.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

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:

A. Notwithstanding any other provision of law, the provisions of this act shall be the exclusive state law for licensees subject to the jurisdiction of the Insurance Commissioner for data security, the investigation of a cybersecurity event, and notification to the Commissioner.

B. This act shall not be construed to create or imply a private cause of action for violations of its provisions.

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:

As used in this act:

1. "Authorized individual" means an individual known to and 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;

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

9 4. "Cybersecurity event" means an event resulting in  
10 unauthorized access to or disruption or misuse of an information  
11 system or nonpublic information stored on the information system.  
12 The term cybersecurity event shall not include the unauthorized  
13 acquisition of encrypted nonpublic information if the encryption,  
14 process, or key is not also acquired, released, or used without  
15 authorization. Cybersecurity event shall not include an event in  
16 which the licensee has determined that the nonpublic information  
17 accessed by an unauthorized person has not been used or released and  
18 has been returned or destroyed;

19 5. "Department" means the Insurance Department;

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

23 7. "Information security program" means the administrative,  
24 technical, and physical safeguards that a licensee uses to access,

1 collect, distribute, process, protect, store, use, transmit, dispose  
2 of, or otherwise handle nonpublic information;

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

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

16 10. "Multi-factor authentication" means authentication through  
17 verification of at least two (2) of the following types of  
18 authentication factors:

- 19 a. knowledge factors, such as a password,
- 20 b. possession factors, such as a token or text message on  
21 a mobile phone, or
- 22 c. inherence factors, such as a biometric characteristic;

23 11. "Nonpublic information" means electronic information that  
24 is not publicly available and is:

- 1 a. business related information of a licensee, of which  
2 the tampering with or unauthorized disclosure, access,  
3 or use of would cause a material adverse impact to the  
4 business, operations, or security of the licensee,
- 5 b. any information concerning a consumer that, because of  
6 name, number, personal mark, or other identifier, can  
7 be used to identify him or her, in combination with  
8 any one or more of the following data elements:
- 9 (1) social security number,
  - 10 (2) driver license number or nondriver identification  
11 card number,
  - 12 (3) financial account number, credit card number, or  
13 debit card number,
  - 14 (4) any security code, access code, or password that  
15 would permit access to a consumer's financial  
16 account, or
  - 17 (5) biometric records, or
- 18 c. any information or data, except age or gender, in any  
19 form or medium created by or derived from a health  
20 care provider or a consumer that can be used to  
21 identify a particular consumer and that relates to:
- 22 (1) the past, present, or future physical, mental, or  
23 behavioral health or condition of any consumer or  
24 a member of the family of the consumer,

- 1 (2) the provision of health care to any consumer, or
- 2 (3) payment for the provision of health care to any
- 3 consumer;

4 12. "Person" means any individual or any nongovernmental  
5 entity including but not limited to any nongovernmental  
6 partnership, corporation, branch, agency, or association;

7 13. "Publicly available information" means any information that  
8 a licensee has reasonable basis to believe is lawfully made  
9 available to the general public from federal, state, or local  
10 government records, widely distributed media, or disclosures to the  
11 general public that are required to be made by federal, state, or  
12 local law. For the purposes of this definition, a licensee has a  
13 reasonable basis to believe that information is lawfully made  
14 available to the general public if the licensee has taken steps to  
15 determine:

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

21 14. "Third-party service provider" means a person, not  
22 otherwise defined as a licensee, that contracts with a licensee to  
23 maintain, process, store, or otherwise is permitted access to

1 nonpublic information through its provision of services to the  
2 licensee.

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

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

16 B. An information security program of a licensee shall be  
17 designed to:

18 1. Protect the security and confidentiality of nonpublic  
19 information and the security of the information systems;

20 2. Protect against any threats or hazards to the security or  
21 integrity of nonpublic information and the information systems;

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

24 and

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

4 C. The licensee shall:

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

8 2. Identify reasonably foreseeable internal or external threats  
9 that could result in unauthorized access, transmission, disclosure,  
10 misuse, alteration, or destruction of nonpublic information  
11 including, but not limited to, the security of information systems  
12 and nonpublic information that are accessible to, or held by, third-  
13 party service providers;

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

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

21 a. employee training and management,

22 b. information systems, including, but not limited to,  
23 network and software design, as well as information  
24



1 classification, governance, processing, storage,  
2 transmission, and disposal, and

3 c. detecting, preventing, and responding to attacks,  
4 intrusions, or other systems failures; and

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

9 D. Based on the results of the risk assessment, the licensee  
10 shall:

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

17 2. Determine and implement security measures deemed  
18 appropriate, including:

19 a. place access controls on information systems  
20 including controls to authenticate and permit access  
21 only to authorized individuals to protect against the  
22 unauthorized acquisition of nonpublic information,  
23 b. identify and manage the data, personnel, devices,  
24 systems, and facilities that enable the organization

1 to achieve business purposes in accordance with their  
2 relative importance to business objectives and the  
3 risk strategy of the organization,

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

6 d. protect by encryption or other appropriate means, all  
7 nonpublic information while being transmitted over an  
8 external network and all nonpublic information stored  
9 on a laptop computer or other portable computing or  
10 storage device or media,

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

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

15 g. utilize effective controls, which may include multi-  
16 factor authentication procedures for any authorized  
17 individual accessing nonpublic information,

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

21 i. include audit trails within the information security  
22 program designed to detect and respond to  
23 cybersecurity events and designed to reconstruct  
24

- 1 material financial transactions sufficient to support  
2 normal operations and obligations of the licensee,  
3 j. implement measures to protect against destruction,  
4 loss, or damage of nonpublic information due to  
5 environmental hazards such as fire and water damage or  
6 other catastrophic events or technological failures,  
7 and  
8 k. develop, implement, and maintain procedures for the  
9 secure disposal of nonpublic information in any format;

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

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

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

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

22 1. Require the executive management of the licensee or 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 to the Insurance Commissioner in writing, at  
3 least annually, the following information:

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

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

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

1 information that are accessible to, or held by, the third-party  
2 service provider.

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

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

17 The incident response plan shall address the following areas:

- 18 1. The internal process for responding to a cybersecurity  
19 event;
- 20 2. The goals of the incident response plan;
- 21 3. The definition of clear roles, responsibilities, and levels  
22 of decision-making authority;
- 23 4. External and internal communications and information  
24 sharing;

1           5. Identification of requirements for the remediation of any  
2 identified weaknesses in information systems and associated  
3 controls;

4           6. Documentation and reporting regarding cybersecurity events  
5 and related incident response activities; and

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

8           I. Annually, each insurer domiciled in this state shall submit  
9 to the Commissioner a written statement by March 1, certifying that  
10 the insurer complies with the requirements set forth in this section.  
11 Each insurer shall maintain, for examination by the Insurance  
12 Department, all records, schedules, and data supporting this  
13 certificate for a period of five (5) years. To the extent an  
14 insurer has identified areas, systems, or processes that require  
15 material improvement, updating, or redesign, the insurer shall  
16 document the identification and the remedial efforts planned and  
17 underway to address such areas, systems, or processes. The  
18 documentation shall be available for inspection by the Commissioner  
19 upon request.

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

23           A. If the licensee learns that a cybersecurity event has or  
24 may have occurred, the licensee, or an outside vendor or service

1 provider designated to act on behalf of the licensee, shall conduct  
2 a prompt investigation.

3 B. During the investigation, the licensee, or an outside vendor  
4 or service provider designated to act on behalf of the licensee,  
5 shall, at a minimum:

6 1. Determine whether a cybersecurity event has occurred;

7 2. Assess the nature and scope of the cybersecurity event;

8 3. Identify any nonpublic information that may have been  
9 involved in the cybersecurity event; and

10 4. Perform or oversee reasonable measures to restore the  
11 security of the information systems compromised in the cybersecurity  
12 event in order to prevent further unauthorized acquisition, release,  
13 or use of nonpublic information in the possession, custody, or  
14 control of the licensee.

15 C. If the licensee learns that a cybersecurity event has or may  
16 have occurred in a system maintained by a third-party service  
17 provider, the licensee shall complete the steps listed in subsection  
18 B of this section or confirm and document that the third-party  
19 service provider has completed those steps.

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

24

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

4 A. Every licensee shall notify the Insurance Commissioner  
5 without unreasonable delay, but not later than three business days,  
6 from a determination that a cybersecurity event involving nonpublic  
7 information that is in the possession of a licensee has occurred  
8 when either of the following criteria has been met:

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

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

20 a. a cybersecurity event impacting the licensee of which  
21 notice is required to be provided to any government  
22 body, self-regulatory agency, or any other supervisory  
23 body pursuant to any state or federal law, or  
24



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

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

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

6           B.    The licensee making the notification required in subsection  
7   A of this section shall provide as much of the following information  
8   as possible, electronically in the manner and form prescribed by the  
9   Commissioner, along with any applicable fees. The licensee shall  
10   have a continuing obligation to update and supplement initial and  
11   subsequent notifications to the Commissioner regarding material  
12   changes to previously provided information relating to the  
13   cybersecurity event. The licensee shall provide:

14           1.    Date of the cybersecurity event;

15           2.    Description of how the information was exposed, lost,  
16   stolen, or breached including, but not limited to, the specific  
17   roles and responsibilities of third-party service providers, if any;

18           3.    How the cybersecurity event was discovered;

19           4.    Whether any lost, stolen, or breached information has been  
20   recovered and, if so, how this was done;

21           5.    The identity of the source of the cybersecurity event;

22           6.    Whether the licensee has filed a police report or has  
23   notified any regulatory, government, or law enforcement agencies  
24   and, if so, when such notification was provided;

1           7. Description of the specific types of information acquired  
2 without authorization. The term "specific types of information"  
3 means particular data elements including, but not limited to, types  
4 of medical information, financial information, or information  
5 allowing identification of the consumer;

6           8. The period during which the information system was  
7 compromised by the cybersecurity event;

8           9. The number of total consumers in this state affected by the  
9 cybersecurity event. The licensee shall provide the best estimate  
10 in the initial report to the Commissioner and update this estimate  
11 with each subsequent report to the Commissioner pursuant to this  
12 section;

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

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

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

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

23           C. A licensee shall comply with the procedures of the Security  
24 Breach Notification Act, Section 161 et seq. of Title 24 of the

1 Oklahoma Statutes, to notify affected consumers and provide a copy  
2 of the notice sent to consumers under that statute to the  
3 Commissioner, when a licensee is required to notify the Commissioner  
4 under subsection A of this section.

5 D. 1. In the case of a cybersecurity event in a system  
6 maintained by a third-party service provider, of which the licensee  
7 has become aware, the licensee shall treat the event as it would  
8 under subsection A of this section unless the third-party service  
9 provider provides the notice required under subsection A of this  
10 section to the Commissioner and the licensee.

11 2. The computation of deadlines of the licensee shall begin on  
12 the day after the third-party service provider notifies the licensee  
13 of the cybersecurity event or the licensee otherwise has actual  
14 knowledge of the cybersecurity event, whichever is sooner.

15 3. Nothing in this act shall prevent or abrogate an agreement  
16 between a licensee and another licensee, a third-party service  
17 provider, or any other party to fulfill any of the investigation  
18 requirements impose or notice requirements imposed under this act.

19 E. 1. In the case of a cybersecurity event involving nonpublic  
20 information that is used by the licensee that is acting as an  
21 assuming insurer, or in the possession, custody, or control of a  
22 licensee, that is acting as an assuming insurer and that does not  
23 have a direct contractual relationship with the affected consumers,  
24 the assuming insurer shall notify its affected ceding insurers and

1 the Commissioner of its state of domicile within three (3) business  
2 days of making the determination that a cybersecurity event has  
3 occurred. The ceding insurers that have a direct contractual  
4 relationship with affected consumers shall fulfill the consumer  
5 notification requirements imposed under the Security Breach  
6 Notification Act, Section 161 et seq. of Title 24 of the Oklahoma  
7 Statutes, and any other notification requirements relating to a  
8 cybersecurity event imposed under this section.

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

22       F. In the case of a cybersecurity event involving nonpublic  
23 information that is in the possession, custody, or control of a  
24 licensee that is an insurer or its third-party service provider for

1 which a consumer accessed the services of the insurer through an  
2 independent insurance producer, and for which consumer notice is  
3 required by this act or the Security Breach Notification Act,  
4 Section 161 et seq. of Title 24 of the Oklahoma Statutes, the  
5 insurer shall notify the producers of record of all affected  
6 consumers of the cybersecurity event no later than the time at which  
7 notice is provided to the affected consumers. The insurer is  
8 excused from this obligation for any producers who are not  
9 authorized by law or contract to sell, solicit, or negotiate on  
10 behalf of the insurer, and in those instances in which the insurer  
11 does not have the current producer of record information for an  
12 individual consumer. Any licensee acting as an assuming insurer  
13 shall have no other notice obligations relating to a cybersecurity  
14 event or other data breach under this section or any other law of  
15 this state.

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

19 A. The Insurance Commissioner shall have power to examine and  
20 investigate the affairs of any licensee to determine whether the  
21 licensee has been or is engaged in any conduct in violation of the  
22 provisions of this act or any rules promulgated thereto. This power  
23 is in addition to the powers which the Commissioner has under  
24 applicable provisions of the Insurance Code including, but not

1 limited to, Sections 309.1 through 309.6, 332, and 1250.4 of Title  
2 36 of the Oklahoma Statutes.

3 B. Whenever the Commissioner has reason to believe that a  
4 licensee has been or is engaged in conduct in this state that  
5 violates any provision of this act, the Commissioner may take action  
6 that is necessary or appropriate to enforce the provisions.

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

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

1 B. Neither the Commissioner nor any person who received  
2 documents, materials, or other information while acting under the  
3 authority of the Commissioner shall be permitted or required to  
4 testify in any private civil action concerning any confidential  
5 documents, materials, or information subject to subsection A of this  
6 section.

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

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

18 2. May receive documents, materials, or information including  
19 otherwise confidential and privileged documents, materials, or  
20 information, from the National Association of Insurance  
21 Commissioners, its affiliates or subsidiaries, and from regulatory  
22 and law enforcement officials of other foreign or domestic  
23 jurisdictions, and shall maintain as confidential or privileged any  
24 document, material, or information received with notice or the

1 understanding that it is confidential or privileged under the laws  
2 of the jurisdiction that is the source of the document, material, or  
3 information;

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

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

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

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

22 F. Documents, materials, or other information in the possession  
23 or control of the National Association of Insurance Commissioners or  
24 a third-party consultant or vendor pursuant to this act shall not be



1 construed to be public information, shall not be subject to the  
2 Oklahoma Open Records Act, shall not be subject to subpoena, and  
3 shall not be subject to discovery or admissible as evidence in any  
4 private civil action.

5 SECTION 9. NEW LAW A new section of law to be codified  
6 in the Oklahoma Statutes as Section 678 of Title 36, unless there is  
7 created a duplication in numbering, reads as follows:

8 A. The Insurance Commissioner may promulgate any rules  
9 necessary to carry out the provisions of this section.

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

11 a. a licensee with less than Five Million Dollars  
12 (\$5,000,000.00) in gross annual revenue, is exempt  
13 from this act,

14 b. a licensee subject to the Health Insurance Portability  
15 and Accountability Act, Pub. L. 104-191, 110 Stat.  
16 1936, as amended, that has established and maintains  
17 an information security program pursuant to such  
18 statutes, rules, regulations, procedures, or  
19 guidelines established thereunder, will be considered  
20 to meet the requirements of Section 4 of this act,  
21 provided that the licensee is compliant with and  
22 submits a written statement to the Commissioner  
23 certifying its compliance with the same, and  
24

1 c. an employee, agent, representative, or designee of a  
2 licensee, who is also a licensee, is exempt from this  
3 act and shall not be required to develop their own  
4 information security program to the extent that the  
5 employee, agent, representative, or designee is  
6 covered by the information security program of the  
7 licensee.

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

11 C. In the case of a violation of this act, a licensee may be  
12 penalized in accordance with any applicable sections of the  
13 Insurance Code, including, but not limited to, Section 908 of Title  
14 36 of the Oklahoma Statutes, or any other provision providing for  
15 penalties that the licensee is subject to under the license or  
16 permit of the licensee. Nothing in this act shall be construed to  
17 impose any civil liability for any violation of this act or omission  
18 to act by the licensee or employees of the licensee.

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

22 SECTION 10. NEW LAW A new section of law to be codified  
23 in the Oklahoma Statutes as Section 679 of Title 36, unless there is  
24 created a duplication in numbering, reads as follows:

1 Licensees shall have one (1) year from the effective date of  
2 this act to implement Section 4 of this act and two (2) years from  
3 the effective date of this act to implement subsection F of Section  
4 4 of this act.

5 SECTION 11. AMENDATORY 51 O.S. 2021, Section 24A.3, as  
6 last amended by Section 1, Chapter 402, O.S.L. 2022 (51 O.S. Supp.  
7 2022, Section 24A.3), is amended to read as follows:

8 Section 24A.3. As used in the Oklahoma Open Records Act:

9 1. "Record" means all documents including, but not limited to,  
10 any book, paper, photograph, microfilm, data files created by or  
11 used with computer software, computer tape, disk, record, sound  
12 recording, film recording, video record or other material regardless  
13 of physical form or characteristic, created by, received by, under  
14 the authority of, or coming into the custody, control or possession  
15 of public officials, public bodies or their representatives in  
16 connection with the transaction of public business, the expenditure  
17 of public funds or the administering of public property. "~~Record~~"

18 Record does not mean:

- 19 a. computer software,
- 20 b. nongovernment personal effects,
- 21 c. unless public disclosure is required by other laws or  
22 regulations, vehicle movement records of the Oklahoma  
23 Transportation Authority obtained in connection with  
24 the Authority's electronic toll collection system,

- 1           d.   personal financial information, credit reports or  
2           other financial data obtained by or submitted to a  
3           public body for the purpose of evaluating credit  
4           worthiness, obtaining a license, permit or for the  
5           purpose of becoming qualified to contract with a  
6           public body,
- 7           e.   any digital audio/video recordings of the toll  
8           collection and safeguarding activities of the Oklahoma  
9           Transportation Authority,
- 10          f.   any personal information provided by a guest at any  
11          facility owned or operated by the Oklahoma Tourism and  
12          Recreation Department to obtain any service at the  
13          facility or by a purchaser of a product sold by or  
14          through the Oklahoma Tourism and Recreation  
15          Department,
- 16          g.   a Department of Defense Form 214 (DD Form 214) filed  
17          with a county clerk including any DD Form 214 filed  
18          before July 1, 2002,
- 19          h.   except as provided for in Section 2-110 of Title 47 of  
20          the Oklahoma Statutes~~7~~7:
- 21               (1) any record in connection with a Motor Vehicle  
22               Report issued by the Department of Public Safety,  
23               as prescribed in Section 6-117 of Title 47 of the  
24               Oklahoma Statutes, or

1 (2) personal information within driver records, as  
2 defined by the Driver's Privacy Protection Act,  
3 18 United States Code, Sections 2721 through  
4 2725, which are stored and maintained by the  
5 Department of Public Safety, ~~or~~

6 i. any portion of any document or information provided to  
7 an agency or entity of the state or a political  
8 subdivision to obtain licensure under the laws of this  
9 state or a political subdivision that contains an  
10 applicant's personal address, personal phone number,  
11 personal electronic mail address or other contact  
12 information. Provided, however, lists of persons  
13 licensed, the existence of a license of a person, or a  
14 business or commercial address, or other business or  
15 commercial information disclosable under state law  
16 submitted with an application for licensure shall be  
17 public record, or

18 j. information relating to a cybersecurity event reported  
19 to the Insurance Commissioner pursuant to the  
20 Insurance Data Security Act;

21 2. "Public body" shall include, but not be limited to, any  
22 office, department, board, bureau, commission, agency, trusteeship,  
23 authority, council, committee, trust or any entity created by a  
24 trust, county, city, village, town, township, district, school

1 district, fair board, court, executive office, advisory group, task  
2 force, study group or any subdivision thereof, supported in whole or  
3 in part by public funds or entrusted with the expenditure of public  
4 funds or administering or operating public property, and all  
5 committees, or subcommittees thereof. Except for the records  
6 required by Section 24A.4 of this title, ~~"public body"~~ public body  
7 does not mean judges, justices, the Council on Judicial Complaints,  
8 the Legislature or legislators. ~~"Public body"~~ Public body shall not  
9 include an organization that is exempt from federal income tax under  
10 Section 501(c)(3) of the Internal Revenue Code of 1986, as amended,  
11 and whose sole beneficiary is a college or university, or an  
12 affiliated entity of the college or university, that is a member of  
13 The Oklahoma State System of Higher Education. Such organization  
14 shall not receive direct appropriations from the Oklahoma  
15 Legislature. The following persons shall not be eligible to serve  
16 as a voting member of the governing board of the organization:

- 17 a. a member, officer, or employee of the Oklahoma State  
18 Regents for Higher Education,
- 19 b. a member of the board of regents or other governing  
20 board of the college or university that is the sole  
21 beneficiary of the organization, or
- 22 c. an officer or employee of the college or university  
23 that is the sole beneficiary of the organization;

24

1        3. "Public office" means the physical location where public  
2 bodies conduct business or keep records;

3        4. "Public official" means any official or employee of any  
4 public body as defined herein; and

5        5. "Law enforcement agency" means any public body charged with  
6 enforcing state or local criminal laws and initiating criminal  
7 prosecutions including, but not limited to, police departments,  
8 county sheriffs, the Department of Public Safety, the Oklahoma State  
9 Bureau of Narcotics and Dangerous Drugs Control, the Alcoholic  
10 Beverage Laws Enforcement Commission, and the Oklahoma State Bureau  
11 of Investigation.

12        SECTION 12. This act shall become effective November 1, 2023.

13        Passed the Senate the 20th day of March, 2023.

14

15

\_\_\_\_\_  
Presiding Officer of the Senate

16

17        Passed the House of Representatives the \_\_\_\_ day of \_\_\_\_\_,

18 2023.

19

20

\_\_\_\_\_  
Presiding Officer of the House  
of Representatives

21

22

23

24