ENGROSSED HOUSE
BILL NO. 2790 By: Stinson of the House

and

Howard of the Senate

An Act relating to cybersecurity; creating The Oklahoma Hospital Cybersecurity Protection Act of 2023; providing definitions; creating requirements for affirmative defense; recognizing industry framework; providing for severability; providing for codification; and providing an 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 2068 of Title 18, unless there is created a duplication in numbering, reads as follows:

This act shall be known and may be cited as "The Oklahoma Hospital Cybersecurity Protection Act of 2023".

SECTION 2. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 2069 of Title 18, unless there is created a duplication in numbering, reads as follows:

As used in this act:

A. "Covered entity" means any hospital, as defined in Section 1-701 of Title 63 of the Oklahoma Statutes, whether for profit or

not-for-profit, which is owned, either in whole in or part, or is managed in whole or in part, by hospitals whose business is subject to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

B. "Data breach" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information or restricted information maintained by a covered entity as part of a database of personal information or restricted information regarding multiple individuals and that causes, or the covered entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. Good-faith acquisition of personal information or restricted information by an employee or agent of a covered entity for the purposes of the covered entity is not a breach of the security system; provided, that the personal information or restricted information, as the case may be, is not used for a purpose other than a lawful purpose of the covered entity or subject to further unauthorized disclosure.

C. "Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted:

1. Social Security number;

2. Driver license number or state identification number issued in lieu of a driver license; or

3. Financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of an individual.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the public.

D. "Restricted information" means any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property.

E. As used in this act, the terms "encrypted" and "redacted" have the same meanings as in Section 162 of Title 24 of the Oklahoma Statutes.

SECTION 3. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 2070 of Title 18, unless there is created a duplication in numbering, reads as follows:

A. The requirements of this section are voluntary; provided, a covered entity may only seek an affirmative defense under this act if the following conditions are met:

1. A covered entity seeking an affirmative defense under this act shall create, maintain, and comply, including documentation of such compliance, with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry-recognized cybersecurity framework, as described in this section.

2. A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in paragraph 1 of subsection A of this section, as applicable:

a. protect the security and confidentiality of the information,

b. protect against any anticipated threats or hazards to the security or integrity of the information, and

c. protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

3. The scale and scope of a covered entity's cybersecurity program under subsection A of this section is appropriate if it is based on all of the following factors:

a. the size and complexity of the covered entity,

b. the nature and scope of the activities of the covered entity,

c. the sensitivity of the information to be protected,

d. the cost and availability of tools to improve information security and reduce vulnerabilities, and

e. the resources available to the covered entity.

4. The cybersecurity program shall contain requirements that it be reviewed, evaluated, and updated on at least an annual basis and shall require documentation of the same.

B. A covered entity that satisfies paragraphs 1 through 4 of subsection A of this section is entitled to an affirmative defense to any cause of action sounding in tort that is brought alleging that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.

SECTION 4. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 2071 of Title 18, unless there is created a duplication in numbering, reads as follows:

A covered entity's cybersecurity program, as described in Section 2 of this act, reasonably conforms to an industry-recognized cybersecurity framework for purposes of that section if subsection A of this section is satisfied:

A. 1. The covered entity is subject to the requirements of the laws or regulations listed below, and the cybersecurity program reasonably conforms to the entirety of the current version of both of the following, subject to paragraph 2 of subsection A of this section:

a. the security requirements of the "Health Insurance Portability and Accountability Act of 1996", as set forth in 45 CFR Part 164 Subpart C; and

b. the "Health Information Technology for Economic and Clinical Health Act", as set forth in 45 CFR Part 162.

2. When a framework listed in paragraph 1 of subsection A of this section is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the amended framework not later than one (1) year after the effective date of the amended framework.

SECTION 5. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 2072 of Title 18, unless there is created a duplication in numbering, reads as follows:

If any provision of this act or the application thereof to a covered entity is for any reason held to be invalid, the remainder of the provisions under those sections and the application of such provisions to other covered entities shall not be thereby affected.

SECTION 6. This act shall become effective November 1, 2023.

Passed the House of Representatives the 22nd day of March, 2023.

_____
Presiding Officer of the House
of Representatives

Passed the Senate the ____ day of _____, 2023.

_____
Presiding Officer of the Senate