

1 STATE OF OKLAHOMA

2 1st Session of the 59th Legislature (2023)

3 HOUSE BILL 2790

By: Stinson

4
5
6 AS INTRODUCED

7 An Act relating to cybersecurity; creating The
8 Oklahoma Hospital Cybersecurity Protection Act of
9 2023; providing definitions; creating requirements
10 for affirmative defense; recognizing industry
11 framework; clarifying no private right of action;
12 providing for severability; providing for
13 codification; and providing an effective date.

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

15 SECTION 1. NEW LAW A new section of law to be codified
16 in the Oklahoma Statutes as Section 2068 of Title 18, unless there
17 is created a duplication in numbering, reads as follows:

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

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

As used in this act:

23 A. "Covered entity" means any hospital, as defined in Section
24 1-701 of Title 63 of the Oklahoma Statutes, whether for profit or

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

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

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

23 1. Social Security number;

24

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

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

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

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

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

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

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

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

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

- 14 a. protect the security and confidentiality of the
15 information,
- 16 b. protect against any anticipated threats or hazards to
17 the security or integrity of the information,
- 18 c. protect against unauthorized access to and acquisition
19 of the information that is likely to result in a
20 material risk of identity theft or other fraud to the
21 individual to whom the information relates.

22 3. The scale and scope of a covered entity's cybersecurity
23 program under subsection A of this section is appropriate if it is
24 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:

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

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

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

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

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

19 Nothing in this act shall be construed as to provide a private
20 right of action, including a class action, with respect to any act
21 or practice regulated under this act.

22 SECTION 6. NEW LAW A new section of law to be codified
23 in the Oklahoma Statutes as Section 2073 of Title 18, unless there
24 is created a duplication in numbering, reads as follows:

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

5 SECTION 7. This act shall become effective November 1, 2023.

6

7 59-1-5928 MJ 01/04/23

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24