

## 18 Okl. St. § 2070

This document is current with emergency effective legislation through Chapter 300 of the Second Regular Session of the 59th Legislature (2024) with exceptions to Chapter 182.

*Oklahoma Statutes, Annotated by LexisNexis® > Title 18. Corporations (Chs. A — 34) > Chapter 34. Oklahoma Hospital Cybersecurity Protection Act of 2023 (§§ 2068 — 2072)*

### **§ 2070. Covered Entity's Cybersecurity Program**

---

**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 this subsection, 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 this subsection 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; and
- 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.

## History

---

Laws 2023, ch. 84, § 3, effective November 1, 2023.

Oklahoma Statutes, Annotated by LexisNexis®

Copyright © 2024 All rights reserved.