

# **Health Care Cybersecurity and Resiliency Act of 2024**

## **SECTION 1. SHORT TITLE**

States that the Act may be cited as “Health Care Cybersecurity and Resiliency Act of 2024.”

## **SECTION 2. DEFINITIONS**

Defines the following terms: 1) “Agency,” 2) “cybersecurity incident,” 3) “cybersecurity state coordinator,” 4) “Director,” 5) “Healthcare and Public Health Sector,” 6) “Information Sharing and Analysis Organization,” 7) “Information System,” and 8) “Secretary.”

## **SECTION 3. DEPARTMENT COORDINATION WITH THE AGENCY**

Directs the Secretary of Health and Human Services (HHS) to coordinate with the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to improve cybersecurity in the Healthcare and Public Health Sector.

## **SECTION 4. CLARIFYING CYBERSECURITY RESPONSIBILITIES AT HHS**

Designates the Administration for Strategic Preparedness and Response at HHS as the Sector Risk Management Agency for the Healthcare and Public Health center.

## **SECTION 5. CYBERSECURITY INCIDENT RESPONSE PLAN**

Requires the HHS Secretary to develop and implement a cybersecurity incident response plan

## **SECTION 6. BREACH REPORTING PORTAL**

Requires the Secretary of HHS to promulgate updated regulations that require the public display of information on corrective actions and recognized security practices applied by covered entities that have experienced a cybersecurity incident or breach.

**SECTION 7. CLARIFYING BREACH REPORTING OBLIGATIONS.** Requires covered entities and business associates to report the number of individuals affected by a cybersecurity incident or breach.

## **SECTION 8. ENHANCING RECOGNITION OF SECURITY PRACTICES**

Requires the Secretary of HHS to issue guidance about how the Department will implement requirements under the Consolidated Appropriations Act of 2021 for deploying recognized security practices for cybersecurity. Requires the issuance of an annual report by the Secretary of HHS about how the Department is complying with this law.

## **SECTION 9. REQUIRED CYBERSECURITY STANDARDS**

Requires the Secretary of HHS to update the Health Insurance Portability and Accountability Act (HIPAA) regulations for HIPAA covered entities and business associates to use modern, up-to-date cybersecurity practices.

## **SECTION 10. GUIDANCE ON RURAL CYBERSECURITY READINESS**

Requires the Secretary of HHS to issue guidance for rural entities and rural health clinics on best practices for cybersecurity breach prevention, resilience, and coordination with federal agencies. Calls for The Government Accountability Office to submit a report to congress on the guidance implementation not later than three years after the enactment of the Health Care Cybersecurity and Resiliency Act of 2024.

## **SECTION 11. GRANTS TO ENHANCE CYBERSECURITY IN THE HEALTH AND**

## **PUBLIC HEALTH SECTORS**

Allows the Secretary of HHS to award grants to eligible entities for the adoption and use of cybersecurity best practices. Eligible entities include: hospitals, cancer centers, rural health clinics, health facilities operated by the Indian Health Service, academic health centers, or a nonprofit entity that enters into a partnership with an eligible entity.

## **SECTION 12. HEALTHCARE CYBERSECURITY WORKFORCE**

Requires the Secretary of HHS, in coordination with the CISA Cybersecurity State Coordinators and private sector health care experts, to provide training to health and public health sector asset owners and operators. Requires the Administrator of the Health Resources and Services Administration to coordinate with CISA to develop a strategic plan to support and promote cybersecurity literacy and expertise within the health care workforce.

