I

118TH CONGRESS
2D SESSION

H. R. 10455

To direct the Secretary of Health and Human Services to establish the Health Sector Cybersecurity Coordination Center, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 17, 2024

Ms. KELLY of Illinois introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committees on Ways and Means, and Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To direct the Secretary of Health and Human Services to establish the Health Sector Cybersecurity Coordination Center, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Healthcare Cybersecurity Improvement Act''.

SEC. 2 FINDINGS.

Congress finds that—

(1) the Department of Health and Human Services found that ransomware attacks on hospitals have more than doubled from 2019 to 2020, with more than 239,000,000 attacks attempted;

(2) in 2020, over 630 health care organizations were subject to data breaches, leading to over 29,000,000 health records publicly released; and

(3) studies indicate that attacks on our nation's health care systems will only increase as hospitals are forced to balance health care costs with an increasingly digital health care system.

SEC. 3 HEALTH SECTOR CYBERSECURITY COORDINATION CENTER.

(a) ESTABLISHMENT.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Health and Human Services (in this Act referred to as the ''Secretary'') shall, in consultation, as appropriate, with other relevant officials within the Department of Health and Human Services, including the Commissioner of Food and Drugs, the Assistant Secretary for Preparedness and Response, and the Officer for Civil Rights and Civil Liberties, establish a center for purposes of coordinating cybersecurity across the health care sector to be known as the Health Sector Cybersecurity Coordination Center (in this section referred to as the ''Center'').

(b) DUTIES.—The Center shall—

(1) support the defense of the information technology infrastructure of the health care sector, including by—

(A) strengthening coordination and information sharing within the sector; and

(B) developing a plan to protect, detect, respond to, and recover from cybersecurity risks and incidents, including for entities with limited technical capacity; and

(2) develop and support technical capabilities and provide advice regarding the development of standards, to prevent and mitigate cyber attacks, including—

(A) the Commissioner of Food and Drugs; and

(B) the Assistant Secretary for Preparedness and Response.

SEC. 4 HEALTH CARE CYBERSECURITY GRANT PROGRAM.

(a) ESTABLISHMENT.—Not later than 1 year after the date of the enactment of this Act, the Secretary shall establish a program to be known as the Health Care Cybersecurity Grant Program for the purpose of awarding grants to eligible entities to obtain equipment and soft-

ware and hire information technology staff to ensure the protection of critical information systems.

(b) GRANT AMOUNT.—Not later than 90 days after funds are made available to carry out this section, the Secretary shall publish the maximum amount of a grant available under this section, as determined by the Secretary.

(c) REPORT.—Not later than 5 years after the date of the enactment of this Act, the Secretary shall prepare and submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the activities and outcomes of the grant program under this section.

(d) DEFINITIONS.—In this section:

(1) ELIGIBLE ENTITY.—The term ''eligible entity'' means a—

(A) hospital with fewer than 300 beds for the provision of patient care; or

(B) rural health clinic.

(2) HOSPITAL.—The term ''hospital'' means a hospital, as defined in section 1861(e) of the Social Security Act (42 U.S.C. 1395x(e)), or a critical access hospital, as defined in section 1861(mm)(1) of such Act (42 U.S.C. 1395x(mm)(1)).

(3) RURAL HEALTH CLINIC.—The term ''rural health clinic'' has the meaning given such term in section 1861(aa) of the Social Security Act (42 U.S.C. 1395x(aa)(2)).

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $100,000,000 for fiscal year 2022, to remain available through fiscal year 2023.

SEC. 5. STANDARDS FOR MEDICAL DEVICES AND INFORMATION SECURITY NETWORKS IN HOSPITALS.

(a) ESTABLISHMENT.—Not later than 1 year after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the heads of appropriate Federal agencies, shall develop standards for the protection of information security networks and digital medical devices in hospitals.

(b) CONSIDERATION.—In developing standards under subsection (a), the Director shall take into consideration—

(1) current Federal standards and guidelines, including—

(A) standards and guidelines developed under section 4 of the Internet of Things Cy-

bersecurity Improvement Act of 2020 (15 U.S.C. 278g–b);

(B) standards promulgated under section 405(d) of the Cybersecurity Act of 2015 (6 U.S.C. 1533); and

(C) standards developed by the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security with respect to critical infrastructure (as defined in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)); and

(2) general security practices, including—

(A) network segmentation between medical devices and patient information; and

(B) the methods used to detect medical devices connected to the internal network of a hospital.

(c) ENFORCEMENT UNDER MEDICARE AND MEDICAID.—

(1) MEDICARE.—Section 1866(a)(1) of the Social Security Act (42 U.S.C. 1395cc(a)(1)) is amended—

(A) in subparagraph (X), by striking ''and'' at the end;

(B) in subparagraph (Y)(ii)(V), by striking the period and inserting ", and"; and

(C) by inserting after subparagraph (Y) the following new subparagraph:

"(Z) in the case of a hospital or a critical access hospital, beginning on the date that is 2 years after the date of the enactment of this subparagraph, to comply with the standards developed under section 5(a) of the Healthcare Cybersecurity Improvement Act.".

(2) MEDICAID.—Section 1902(a) of the Social Security Act (42 U.S.C. 1396a(a)) is amended—

(A) in paragraph (86), by striking "and" at the end;

(B) in paragraph (87)(D), by striking the period and inserting "; and"; and

(C) by inserting after paragraph (87) the following new paragraph:

"(88) provide that, beginning on the date that is 2 years after the date of the enactment of this paragraph, no hospital be eligible to participate under the plan (or a waiver of such plan) unless such hospital complies with the standards developed under section 5(a) of the Healthcare Cybersecurity Improvement Act.".

(d) QUINQUENNIAL REVIEW AND REVISION.—Not later than 5 years after the date on which the Secretary publishes the standards under subsection (a), and not less frequently than once every 5 years thereafter, the Secretary, shall review and revise such standards, as appropriate.

SEC. 6. LIMITATION ON LIABILITY FOR A LARGE HOSPITAL.

(a) IN GENERAL.—Notwithstanding any other provision of law, a large hospital shall not be liable in any covered civil action to a smaller health entity if such hospital provided cybersecurity assistance to such entity with respect to electronic data, unless such entity can prove by clear and convincing evidence that the alleged harm was caused by gross negligence or willful misconduct.

(b) EXCEPTION.—For purposes of this section, any acts or omissions by a large hospital resulting from a resource or staffing shortage shall not be considered willful misconduct or gross negligence.

(c) DEFINITIONS.—In this section:

(1) COVERED CIVIL ACTION.—The term ''covered civil action'' means a civil action under State law from harm resulting from the acquisition, storage, security, use, misuse, disclosure, or transmission of electronic data of any kind, including—

(A) information security and privacy;

(B) penalties, including for regulatory defense;

(C) misuse of website media content; and

(D) disclosure, misuse, or improper (or inadequate) storage or security of personal and confidential information.

(2) LARGE HOSPITAL.—The term ''large hospital'' means a hospital with 300 or more beds for the provision of patient care.

(3) HOSPITAL.—The term ''hospital'' has the meaning given such term in section 1861(e) of the Social Security Act (42 U.S.C. 1395x).

(4) RURAL HEALTH CLINIC.—The term ''rural health clinic'' has the meaning given such term in section 1861(aa) of the Social Security Act (42 U.S.C. 1395x(aa)(2)).

(5) SMALL HEALTH ENTITY.—The term ''small health entity'' means—

(A) a hospital with fewer than 299 beds for the provision of patient care; and

(B) a rural health clinic.

○