118TH CONGRESS
2D SESSION

S. 5218

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 25, 2024

Mr. WYDEN (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Finance

---

A BILL

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, 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; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Health Infrastructure Security and Accountability Act of 2024''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—STRENGTHENING AND INCREASING OVERSIGHT OF, AND COMPLIANCE WITH, SECURITY STANDARDS FOR HEALTH INFORMATION

SEC. 101. SECURITY REQUIREMENTS.

(a) IN GENERAL.—Section 1173(d)(1) of the Social Security Act (42 U.S.C. 1320d–2(d)(1)) is amended—

(1) in subparagraph (A), by redesignating clauses (i) through (v) as subclauses (I) through (V) respectively and indenting appropriately;

(2) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii) respectively and indenting appropriately;

(3) by striking ''SECURITY STANDARDS.—The Secretary'' and inserting the following: ''MINIMUM SECURITY STANDARDS.—

''(A) IN GENERAL.—The Secretary'';

(4) in subparagraph (A), as added by paragraph (3)—

(A) in clause (i)(V), by striking ''and'' at the end;

(B) in clause (ii), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following new clause:

''(iii) include minimum and enhanced security requirements adopted under subparagraph (B)''; and

(5) by adding at the end the following new subparagraph:

''(B) MINIMUM AND ENHANCED SECURITY REQUIREMENTS.—

''(i) ADOPTION.—Subject to clauses (iii) and (iv), in order to protect health information, protect patient safety, and ensure the availability and resiliency of health care information systems and health

care transactions, the Secretary shall adopt—

"(I) minimum security requirements for covered entities and business associates; and

"(II) enhanced security requirements for covered entities and business associates that—

"(aa) are of systemic importance, as determined by the Secretary; or

"(bb) are important to national security, as determined by the Secretary, in consultation with the Director of Cybersecurity and Infrastructure Security Agency and the Director of National Intelligence.

"(ii) APPLICATION OF ENHANCED SECURITY REQUIREMENTS.—

"(I) NOTIFICATION.—The Secretary shall, at a time and in a manner determined appropriate by the Secretary, notify each covered entity and business associate that is subject

to the enhanced security requirements under clause (i)(II).

''(II) LIMITATION ON REVIEW.—There shall be no administrative or judicial review under section 1869, 1878, or otherwise of the methodology the Secretary uses to determine whether a covered entity or business associate is subject to the enhanced security requirements under clause (i)(II).

''(iii) FACTORS.—In addition to the factors described in subparagraph (A)(i), in developing—

''(I) the minimum security requirements under clause (i)(I), the Secretary shall, in consultation with the Director of Cybersecurity and Infrastructure Security Agency and the Director of National Intelligence, design the requirements to prevent—

''(aa) cyber incidents utilizing the tools and strategies used to target covered entities or business associates;

"(bb) the potential harms, as defined by the Secretary, to national security that could result from a cyber incident involving a covered entity or business associate;

"(cc) the potential harms, as defined by the Secretary, to patients that could result from a cyber incident involving a covered entity or business associate; and

"(dd) other potential harms from cyber incidents, as determined appropriate by the Secretary; and

"(II) the enhanced security requirements under clause (i)(II), the Secretary shall, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of National Intelligence, design the requirements to prevent the potential harms described in subclause (I) and protect against the specific threats the covered entities and

business associates described in such clause face.

''(iv) REVIEW AND UPDATE OF REQUIREMENTS.—The Secretary shall review and update the minimum and enhanced security requirements adopted under clause (i) not less frequently than every 2 years.

''(v) EFFECTIVE DATE AND RULEMAKING.—

''(I) EFFECTIVE DATE.—The requirements under this subparagraph shall take effect on the date that is 2 years after the date of enactment of this subparagraph.

''(II) RULEMAKING.—Not later than 18 months after the date of enactment of this subparagraph, the Secretary shall promulgate regulations to carry out this subparagraph.

''(vi) DEFINITIONS.—For purposes of this subsection:

''(I) BUSINESS ASSOCIATE.—The term 'business associate' has the meaning given such term in section 160.103 of title 45, Code of Federal

Regulations (or a successor regulation).

''(II) COVERED ENTITY.—The term 'covered entity' has the meaning given that term in section 160.103 of title 45, Code of Federal Regulations (or a successor regulation).

''(III) SYSTEMIC IMPORTANCE.—The term 'systemic importance' means, with respect to a covered entity or business associate, that the failure of, or a disruption to, such entity or associate would have a debilitating impact on access to health care or the stability of the health care system of the United States (as determined by the Secretary).''.

(b) AVAILABILITY OF HEALTH INFORMATION.—Section 1173(d)(2)(A) of the Social Security Act (42 U.S.C. 1320d–2(d)(2)(A)) is amended by striking ''the integrity and confidentiality'' and inserting ''the availability, integrity, and confidentiality.

SEC. 102. SECURITY RISK MANAGEMENT, REPORTING REQUIREMENTS, AND AUDITS FOR COVERED ENTITIES AND BUSINESS ASSOCIATES.

(a) SECURITY RISK MANAGEMENT AND REPORTING.—Section 1173(d) of the Social Security Act (42 U.S.C. 1320d–2(d)) is amended by adding at the end the following new paragraph:

"(3) SECURITY RISK MANAGEMENT AND REPORTING.—

"(A) IN GENERAL.—Each covered entity and business associate shall at a minimum, on an annual basis—

"(i) conduct and document a security risk analysis, including information regarding the manner and extent to which such entity or associate is exposed to risk through its business associates;

"(ii) document a plan for a rapid and orderly resolution in the event of a natural disaster, disruptive cyber incident, or other technological failure to its information systems or those of its business associates;

"(iii) conduct a stress test to evaluate whether such entity or associate has the capabilities and planning necessary to recover essential functions, such as patient

care operations and transactions described in subsection (a)(2), following a cyber incident, a natural disaster, or other substantial threat to health care operations, as determined by the Secretary;

''(iv) document whether, based upon the results of the stress test described in clause (iii), the covered entity or business associate revised the most recent plan described in clause (ii);

''(v) provide a written statement signed by the chief executive officer and chief information security officer (or equivalent thereof) stating that the covered entity or business associate is in compliance with security requirements adopted under part 160 of title 45, Code of Federal Regulations, and subparts A and C of part 164 of title 45, Code of Federal Regulations (or a successor regulation), including the applicable security requirements adopted under paragraph (1)(B); and

''(vi) publish on a publicly accessible website—

''(I) whether the covered entity or business associate has received a notification from the Secretary pursuant to paragraph (1)(B)(ii)(I);

''(II) whether the covered entity or business associate meets the minimum security requirements and, if applicable, the enhanced security requirements under paragraph (1)(B); and

''(III) a copy of each statement provided under clause (v) with respect to each year in a machine-readable format.

''(B) STRESS TEST METHODOLOGY.—The Secretary shall provide for not less than 2 different sets of conditions under which the test described in subparagraph (A)(iii) is to be conducted.

''(C) WAIVER AUTHORITY.—The Secretary may waive the requirements of this paragraph with respect to a covered entity or business associate if the burden on the entity or associate significantly outweighs the benefits, taking into account the revenue of the entity or associate,

the volume of protected health information or health care transactions processed by the entity or associate, and such other factors as the Secretary determines appropriate.

''(D) REPORTING.—

''(i) IN GENERAL.—Subject to clause (ii), each covered entity and business associate shall submit the documentation required under subparagraph (A) at such time, in such form, and containing such information as the Secretary may require.

''(ii) ANNUAL REPORTING FOR COVERED ENTITIES AND BUSINESS ASSOCIATES SUBJECT TO ENHANCED SECURITY REQUIREMENTS.—Each covered entity and business associate that is subject to enhanced security requirements shall submit the documentation required under subparagraph (A) to the Secretary not less frequently than on an annual basis.

''(E) DEFINITIONS.—For purposes of this subsection:

''(i) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2200(12) of the

Homeland Security Act of 2002 (6 U.S.C. 650(12)).

''(ii) MACHINE-READABLE.—The term 'machine-readable' has the meaning given such term in section 3502 of title 44, United States Code.

''(iii) STRESS TEST.—The term 'stress test' means an extensive real-world simulation intended to test the operational resilience of the health care operations of a covered entity or business associate in response to a substantial interruption in information systems, including the ability to—

''(I) continue to provide essential care and services during and in the recovery period from such substantial interruption; and

''(II) timely rebuild the information systems (as defined in section 2200(14) of the Homeland Security Act of 2002 (6 U.S.C. 650(14))) of such covered entity or business associate.

"(F) EFFECTIVE DATE.—The requirements under this paragraph shall take effect on the date that is 3 years after the date of enactment of this paragraph.".

(b) INDEPENDENT SECURITY COMPLIANCE AUDITS.—Section 1173(d) of the Social Security Act (42 U.S.C. 1320d–2(d)), as amended by subsection (a), is amended by adding at the end the following new paragraph:

"(4) INDEPENDENT SECURITY COMPLIANCE AUDITS.—

"(A) IN GENERAL.—Each covered entity and business associate must—

"(i) contract with an independent auditor that meets such requirements for independence and technical expertise as the Inspector General of the Department of Health and Human Services may establish to conduct an annual audit in accordance with subparagraph (B); and

"(ii) document the findings of each audit conducted under clause (i).

"(B) AUDIT REQUIREMENTS.—An audit conducted under subparagraph (A)(i) shall—

"(i) assess compliance of the covered entity or business associate with—

"(I) during the period prior to the effective date of the requirements under paragraph (1)(B), the Healthcare and Public Health Sector Cybersecurity Performance Goals as described in the report published by the Department of Health and Human Services as of the date of enactment of this paragraph, and titled 'Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals: Strengthening the Cybersecurity of the Healthcare Sector and Keeping Patients Safe and Secure'; and

"(II) on or after the effective date of the requirements under paragraph (1)(B), the minimum and enhanced security requirements adopted under such paragraph, as applicable;

"(ii) identify any areas in which the covered entity or business associate did not

meet such goals or requirements, as applicable; and

"(iii) certify that the covered entity or business associate—

"(I) has resolved any areas of noncompliance; or

"(II) is implementing an appropriate plan to resolve such areas of noncompliance in a timely manner.

"(C) WAIVER AUTHORITY.—The Secretary may waive the requirements of this paragraph with respect to a covered entity or business associate if the burden on the entity or associate significantly outweighs the benefits, taking into account the revenue of the entity or associate, the volume of protected health information or health care transactions processed by the entity or associate, and such as other factors as the Secretary determines appropriate.

"(D) REPORTING.—

"(i) IN GENERAL.—Subject to clause (ii), each covered entity and business associate shall submit the documentation required under subparagraph (A)(ii) at such

time, in such form, and containing such information as the Secretary may require.

''(ii) ANNUAL REPORTING FOR ENTITIES AND ASSOCIATES SUBJECT TO ENHANCED SECURITY REQUIREMENTS.—Each covered entity and business associate that is subject to enhanced security requirements shall submit the documentation required under subparagraph (A)(ii) to the Secretary not less frequently than on an annual basis.

''(E) EFFECTIVE DATE.—The requirements under this paragraph shall take effect on the date that is 180 days after the date of enactment of this paragraph.''.

(c) SECRETARIAL AUDITS OF DATA SECURITY PRACTICES.—Section 1173(d) of the Social Security Act (42 U.S.C. 1320d–2(d)), as amended by subsections (a) and (b), is amended by adding at the end the following new paragraph:

''(5) SECRETARIAL AUDITS OF DATA SECURITY PRACTICES.—

''(A) IN GENERAL.—Each year (beginning on or after the date this is 4 years after the date of enactment of this paragraph) the Sec-

retary shall conduct an annual audit of the data security practices of at least 20 covered entities or business associates under this part. The Comptroller General of the United States shall monitor auditing activities conducted under this paragraph.

''(B) CONSIDERATIONS.—In selecting covered entities or business associates for audit under subparagraph (A) the Secretary shall consider—

''(i) whether the covered entity or business associate is of systemic importance;

''(ii) whether any complaints have been made with respect to the data security practices of the covered entity or business associate; and

''(iii) whether the covered entity or business associate has a history of previous violations.

''(C) CORRECTIVE ACTION PLAN AND PENALTIES.—The findings of an audit under this paragraph may result in a civil money penalty based on the failure of a covered entity or business associate to submit documentation dem-

onstrating that the covered entity or business associate has taken corrective actions to achieve compliance in response to a finding of a potential violation of a provision of this part within a period of time specified by the Secretary after receipt of such findings.

''(D) REPORTS TO CONGRESS.—The Secretary shall submit to Congress reports summarizing the results of the audits conducted under this paragraph biennially ending on the date that is 10 years after the date on which the first report is submitted under this subparagraph.''.

(d) CIVIL AND CRIMINAL PENALTIES FOR FAILURE TO COMPLY WITH DOCUMENTATION, REPORTING, AND AUDIT REQUIREMENTS.—Section 1173(d) of the Social Security Act (42 U.S.C. 1320d–2(d)), as amended by subsections (a), (b), and (c), is amended by adding at the end the following new paragraph:

''(6) CIVIL AND CRIMINAL PENALTIES FOR FAILURE TO COMPLY WITH DOCUMENTATION, REPORTING, AND AUDIT REQUIREMENTS.—

''(A) CIVIL PENALTIES.—

''(i) IN GENERAL.—A covered entity or business associate that—

"(I) fails to timely submit documentation or a report required under paragraph (3), (4), or (5),

"(II) fails to comply with an audit under paragraph (5), or

"(III) fails to comply with a responsibility of a covered entity or a business associate under section 160.310 of title 45, Code of Federal Regulations (or a successor regulation),

shall be subject to a civil money penalty of not more than $5,000 per day for each such failure.

"(ii) PROCEDURES.—The provisions of section 1128A (other than subsections (a), (b), and (d)(1), and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subparagraph in the same manner as such provisions apply to the imposition of a penalty under such section 1128A.

"(iii) CLARIFICATION.—Any civil money penalty under this subparagraph with respect to a failure described in clause

(i) shall be in lieu of the penalties described in section 1176.

''(B) CRIMINAL PENALTIES.—In addition to any penalties imposed under subparagraph (A), whoever submits, or causes to be submitted, any documentation or report required of a covered entity or business associate under paragraph (3), (4), or (5) knowing that such documentation or report contains false information, or willfully fails to timely submit, or willfully causes to not be timely submitted, such a document or report, shall be guilty of a felony and upon conviction thereof fined not more than $1,000,000 or imprisoned for not more than 10 years, or both.''.

SEC. 103. INCREASED CIVIL PENALTIES FOR FAILURE TO COMPLY WITH SECURITY STANDARDS AND REQUIREMENTS FOR HEALTH INFORMATION.

(a) INCREASED CIVIL PENALTIES.—Section 1176 of the Social Security Act (42 U.S.C. 1320d–5) is amended—

(1) in subsection (a)(1), in the matter preceding subparagraph (A), by striking ''subsection (b)'' and inserting ''subsections (b) and (d)'';

(2) by redesignating subsections (d) and (e) as subsections (e) and (f); and

(3) by inserting after subsection (c) the following new subsection:

''(d) SPECIAL RULES FOR FAILURE TO COMPLY WITH SECURITY STANDARDS AND REQUIREMENTS FOR HEALTH INFORMATION.—

''(1) IN GENERAL.—In the case of a violation of the security standards and requirements under section 1173(d) that occurs after the effective date of the requirements under paragraph (1)(B) of such section, the following rules shall apply:

''(A) Subsection (a)(1)(A) shall be applied by substituting 'that is at least $500' for 'that is at least the amount described in paragraph (3)(A) but not to exceed the amount described in paragraph (3)(D)'.

''(B) Subsection (a)(1)(B) shall be applied by substituting 'that is at least $5,000' for 'that is at least the amount described in paragraph (3)(B) but not to exceed the amount described in paragraph (3)(D)'.

''(C) Subsection (a)(1)(C)(i) shall be applied by substituting 'that is at least $50,000' for 'that is at least the amount described in

paragraph (3)(C) but not to exceed the amount described in paragraph (3)(D)'.

''(D) Subsection (a)(1)(C)(ii) shall be applied by substituting 'that is at least $250,000' for 'that is at least the amount described in paragraph (3)(D)'.

''(E) In addition to the factors described in the second sentence of subsection (a)(1), in determining the amount of a penalty under this section for a violation of the security standards and requirements under section 1173(d), the Secretary shall also base such determination on—

''(i) the size of the covered entity or business associate (as such terms are defined in section 1173(d)(1)(B)(vi)) subject to the penalty;

''(ii) the full compliance history of the covered entity or business associate,

''(iii) good faith efforts to comply with the security standards and requirements; and

''(iv) such other matters as the Secretary determines appropriate.

''(F) Subsection (a)(3) shall not apply.

''(2) DISTRIBUTION OF CERTAIN CIVIL MONETARY PENALTIES COLLECTED.—

''(A) IN GENERAL.—Subject to the regulation promulgated pursuant to subparagraph (B), any civil monetary penalty or monetary settlement collected with respect to a violation of the security standards and requirements under section 1173(d) that occurs after the effective date of such requirements under paragraph (1)(B) of such section shall be transferred to the Office for Civil Rights of the Department of Health and Human Services to be used for the purposes of enforcing the provisions of this part and subparts C and E of part 164 of title 45, Code of Federal Regulations (or any successor regulation).

''(B) ESTABLISHMENT OF METHODOLOGY TO DISTRIBUTE PERCENTAGE OF CMPS COLLECTED TO HARMED INDIVIDUALS.—Not later than 18 months after the date of the enactment of this subparagraph, the Secretary shall establish by regulation a methodology under which an individual who is harmed by an act that constitutes a violation referred to in subparagraph (A) may receive a percentage of any civil mone-

tary penalty or monetary settlement collected with respect to such violation.

"(C) APPLICATION OF METHODOLOGY.—The methodology under subparagraph (B) shall be applied to any civil monetary penalty or monetary settlement collected with respect to a violation of the security standards and requirements under section 1173(d) that occurs after the effective date of such requirements under paragraph (1)(B) of such section.".

(b) STRIKING AMENDMENT TO THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT RELATED TO FINES AND AUDITS.—

(1) IN GENERAL.—Part 1 of subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), as amended by Public Law 116–321, is amended by striking section 13412.

(2) EFFECTIVE DATE.—The amendment made by this subsection shall take effect on the date of enactment of this Act, and apply to determinations made on or after such date.

SEC. 104. USER FEE TO SUPPORT DATA SECURITY OVERSIGHT AND ENFORCEMENT ACTIVITIES.

Section 1173(d) of the Social Security Act (42 U.S.C. 1320d–2(d)), as amended by section 102, is amended by adding at the end the following new paragraph:

"(7) USER FEE TO SUPPORT DATA SECURITY OVERSIGHT AND ENFORCEMENT ACTIVITIES.—

"(A) IN GENERAL.—Each covered entity and business associate shall pay the fee established by the Secretary under subparagraph (B).

"(B) AUTHORIZATION.—The Secretary is authorized to charge a fee to each covered entity and business associate that is equal to the pro rata share of the entity or associate (equal to the ratio, as estimated by the Secretary, of the revenue of the entity or associate for the preceding fiscal year to national health expenditures, as determined by the Secretary, for the preceding fiscal year) of the aggregate amount of fees which the Secretary is directed to collect in a fiscal year. Any amounts collected shall be available without further appropriation to the Secretary for the purpose of carrying out oversight and enforcement activities under this subsection.

"(C) LIMITATION.—In any fiscal year (beginning with fiscal year 2026) the fees collected by the Secretary under subparagraph (B) shall not exceed the lesser of—

"(i) the estimated costs to be incurred by the Secretary in the fiscal year in carrying out oversight and enforcement activities under this subsection; or

"(ii)(I) in fiscal year 2026, $40,000,000;

"(II) in fiscal year 2027, $50,000,000; and

"(III) in fiscal year 2028 or a subsequent fiscal year, the amount determined under this clause for the preceding fiscal year, increased by the percentage increase in the consumer price index for all urban consumers (all items; United States city average) over the previous year.".

TITLE II—MEDICARE ASSISTANCE TO ADDRESS CYBERSECURITY INCIDENTS

SEC. 201. MEDICARE SAFE CYBERSECURITY PRACTICES ADOPTION PROGRAM FOR ELIGIBLE HOSPITALS AND CRITICAL ACCESS HOSPITALS.

(a) INCENTIVE PAYMENTS.—Section 1886 of the Social Security Act (42 U.S.C. 1395ww) is amended by adding at the end the following new subsection:

''(u) INCENTIVES FOR ADOPTION OF ESSENTIAL AND ENHANCED CYBERSECURITY PRACTICES.—

''(1) INVESTMENT.—

''(A) FISCAL YEARS 2027 AND 2028.—For fiscal years 2027 and 2028, upon request, a critical access hospital or an eligible high-needs hospital shall be paid from the Federal Hospital Insurance Trust Fund established under section 1817 a proportional share (as determined by the Secretary) of $800,000,000 to adopt essential cybersecurity practices.

''(B) FISCAL YEARS 2029 AND 2030.—For fiscal years 2029 and 2030, upon request, a critical access hospital or an eligible hospital shall be paid from the Federal Hospital Insurance Trust Fund established under section

1817 a proportional share (as determined by the Secretary) of $500,000,000 to adopt enhanced cybersecurity practices.

''(C) FORM OF PAYMENT.—A payment under this subsection may be in the form of a single consolidated payment or in the form of such periodic installments as the Secretary may specify.

''(2) ADOPTION.—

''(A) ESSENTIAL CYBERSECURITY PRACTICES.—Beginning in fiscal year 2029 for an eligible hospital, and in calendar year 2029 for a critical access hospital, such hospital or critical access hospital shall be treated as an adopter of essential cybersecurity practices for a payment year if such hospital or critical access hospital submits information to the Secretary, in a form and manner specified by the Secretary, and in addition to the information required by subsection (n)(3)(A)(iii), attesting to implementation of essential cybersecurity practices selected by the Secretary for the EHR reporting period with respect to such year.

''(B) ENHANCED CYBERSECURITY PRACTICES.—Beginning in fiscal year 2030 for an

eligible hospital, and in calendar year 2030 for a critical access hospital, such hospital or critical access hospital shall be treated as an adopter of enhanced cybersecurity practices for a payment year if such hospital or critical access hospital submits information to the Secretary, in a form and manner specified by the Secretary, and in addition to the information required by subsection (n)(3)(A)(iii), attesting to implementation of enhanced cybersecurity practices selected by the Secretary during the EHR reporting period with respect to such year.

''(C) IDENTIFICATION OF ESSENTIAL CYBERSECURITY PRACTICES.—Beginning in fiscal year 2027, the Secretary shall, through notice and comment rulemaking, identify essential cybersecurity practices for an EHR reporting period that address known vulnerabilities to data infrastructure and patient health information and ensure patient safety and continuity of patient care.

''(D) IDENTIFICATION OF ENHANCED CYBERSECURITY PRACTICES.—Beginning in fiscal year 2028, the Secretary shall, through notice and comment rulemaking, identify enhanced cy-

bersecurity practices for an EHR reporting period that address the safe use of digital data, safety and continuity of patient care, advance cybersecurity resilience across the hospital sector, address high-risk cybersecurity vulnerabilities (as determined by the Secretary), and ensure patient safety and continuity of care.

''(E) UPDATING.—The Secretary may update essential and enhanced cybersecurity practices required under this subsection through notice and comment rulemaking as needed to reflect evolving cybersecurity practices.

''(3) APPLICATION.—

''(A) LIMITATIONS ON REVIEW.—There shall be no administrative or judicial review under section 1869, section 1878, or otherwise, of—

''(i) the methodology and standards for determining payment amounts under this subsection and payment adjustments under subsection (b)(3)(B)(xiii) and section 1814(l)(6)(A);

''(ii) the methodology and standards for determining whether an eligible hos-

pital is an essential or enhanced cybersecurity practices adopter under paragraph (2) and the Secretary's determination of whether or not to apply the hardship exception to an eligible hospital under subsection (b)(3)(B)(xiii)(III); or

"(iii) any alteration by the Secretary of the requirements specified in paragraph (2).

"(B) POSTING ON WEBSITE.—The Secretary shall post on the Internet website of the Centers for Medicare & Medicaid Services, in an easily understandable format, the number by State of eligible hospitals and critical access hospitals that are not essential or enhanced cybersecurity adopters as applicable for a year.

"(4) DEFINITIONS.—For purposes of this subsection:

"(A) EHR REPORTING PERIOD.—The term 'EHR reporting period' means the period determined by the Secretary under subsection (n)(6)(A).

"(B) ELIGIBLE HIGH-NEEDS HOSPITAL.—The term 'eligible high-needs hospital' means an eligible hospital that—

''(i) is a subsection (d) Puerto Rico hospital (as defined in subsection (d)(9)(A));

''(ii) is operated by the Indian Health Service or by an Indian tribe or tribal organization (as those terms are defined in section 4 of the Indian Health Care Improvement Act);

''(iii) has a disproportionate percentage of Medicare beneficiaries who are dually eligible for benefits under this title and title XIX across all subsection (d) hospitals in the baseline period (as specified by the Secretary) of at least 75 percent;

''(iv) has a disproportionate percentage of Medicare beneficiaries who are subsidy eligible individuals (as defined in section 1860D–14(a)(3)) across all subsection (d) hospitals in the baseline period (as specified by the Secretary) of at least 75 percent (as determined by the Secretary under subsection (d)(5)(F)(vi));

''(v) is located in a rural area (as defined in subsection (d)(2)(D));

"(vi) is classified as a rural referral center under subsection (d)(5)(C);

"(vii) is a sole community hospital (as defined in subsection (d)(5)(D)(iii));

"(viii) is a low-volume hospital (as defined in subsection (d)(12)(C)(i)); or

"(ix) is a medicare-dependent, small rural hospital (as defined in subsection (d)(5)(G)).

"(C) ELIGIBLE HOSPITAL.—The term 'eligible hospital' has the meaning given that term in subsection (n)(6)(B).

"(D) ENHANCED CYBERSECURITY PRACTICES.—The term 'enhanced cybersecurity practices' means enhanced security requirements adopted under section 1173(d)(1)(B)(i)(II) and such additional practices as the Secretary may select for a year that are greater than essential cybersecurity practices.

"(E) ESSENTIAL CYBERSECURITY PRACTICES.—The term 'essential cybersecurity practices' means the minimum security requirements adopted under section

1173(d)(1)(B)(i)(I) and such additional practices as the Secretary may select for a year.''.

(b) PAYMENT REDUCTIONS FOR FAILURE TO ADOPT SAFE CYBERSECURITY PRACTICES; SIGNIFICANT HARDSHIP EXCEPTION.—

(1) HOSPITALS.—Section 1886(b)(3)(B) of the Social Security Act (42 U.S.C. 1395ww(b)(3)(B)) is amended by adding at the end the following new clause:

''(xiii)(I) For purposes of clause (i)—

''(aa) for fiscal year 2029, in the case of an eligible hospital that is not an adopter of the essential cybersecurity practices for a payment year (as determined under subsection (u)(2)(A)) for an EHR reporting period for such year, the applicable percentage increase otherwise applicable under clause (i) (determined without regard to clause (viii) or (xi)) for such fiscal year shall be reduced (but not below zero) by 0.25 percentage point;

''(bb) for fiscal year 2030, in the case of an eligible hospital that is not an adopter of the essential cybersecu-

rity practices for a payment year (as determined under subsection (u)(2)(A)) for an EHR reporting period for such year—

"(AA) the applicable percentage increase otherwise applicable under clause (i) (determined without regard to clause (viii) or (xi)) for such fiscal year shall be reduced (but not below zero) by 0.50 percentage point; and

"(BB) the base operating DRG payment amount (as defined in subsection (o)(7)(D)) for such hospital for each discharge in such fiscal year shall be reduced by 0.25 percent;

"(cc) for fiscal year 2031, in the case of an eligible hospital that is not an adopter of the enhanced cybersecurity practices for a payment year (as determined under subsection (u)(2)(B)) for an EHR reporting period for such fiscal year—

"(AA) the applicable percentage increase otherwise applicable under clause (i) (determined without regard to clause (viii) or (xi)) for such fiscal year shall be reduced (but not below zero) by 0.75 percentage point; and

"(BB) the base operating DRG payment amount (as defined in subsection (o)(7)(D)) for such hospital for each discharge in such fiscal year shall be reduced by 0.50 percent;

"(dd) for fiscal year 2032, in the case of an eligible hospital that is not an adopter of the enhanced cybersecurity practices for a payment year (as determined under subsection (u)(2)(B)) for an EHR reporting period for such fiscal year—

"(AA) the applicable percentage increase otherwise applicable under clause (i) (determined without regard to clause

(viii) or (xi)) for such fiscal year shall be reduced (but not below zero) by 1.0 percentage point; and

''(BB) the base operating DRG payment amount (as defined in subsection (o)(7)(D)) for such hospital for each discharge in such fiscal year shall be reduced by 0.75 percent; and

''(ee) for fiscal year 2033 and each subsequent fiscal year, in the case of an eligible hospital that is not an adopter of the enhanced cybersecurity practices for a payment year (as determined under subsection (u)(2)(B)) for an EHR reporting period for such fiscal year—

''(AA) the applicable percentage increase otherwise applicable under clause (i) (determined without regard to clause (viii) or (xi)) for such fiscal year shall be reduced (but not below

zero) by 1.0 percentage point; and

"(BB) the base operating DRG payment amount (as defined in subsection (o)(7)(D)) for such hospital for each discharge in such fiscal year shall be reduced by 1.0 percent.

"(II) A reduction under subclause (I) shall apply only with respect to the fiscal year involved, and the Secretary shall not take into account such reduction in making payments to a hospital under this section in a subsequent fiscal year.

"(III) The Secretary may, on a case-by-case basis, except an eligible hospital from the application of subclause (I) with respect to a fiscal year if the Secretary determines, subject to annual renewal, that requiring such hospital to be an essential or enhanced cybersecurity practices adopter during such fiscal year would result in a significant hardship, such as in the case of a natural disaster, a bankruptcy, limited internet connectivity, an incident (as de-

fined in section 2200 of the Homeland Security Act of 2002) that significantly disrupts medicare claims processing, or any other similar situation that the Secretary determines interfered with the ability of the eligible hospital to meet the requirements. An eligible hospital may not be granted an exemption under this subclause for more than 5 years, except in cases where the Secretary determines such hospital has experienced an incident (as so defined) that significantly disrupts medicare claims processing. The Secretary shall establish an exception process and post an application for an exception on the Internet website of the Centers for Medicare & Medicaid Services. Such process shall require that the application be submitted to the Secretary by not later than 6 months after the conclusion of the EHR reporting period for the relevant year.

''(IV) In the case of a State for which the Secretary has waived all or part of this section under the authority of section 1115A, nothing in this section shall pre-

clude such State from implementing an adjustment similar to the adjustment under subclause (I).

''(V) In this clause, the term 'eligible hospital' has the meaning given such term in subsection (u)(4).''.

(2) CRITICAL ACCESS HOSPITALS.—Section 1814(l) of the Social Security Act (42 U.S.C. 1395f(l)) is amended—

(A) by redesignating paragraph (5) as paragraph (6);

(B) by inserting after paragraph (4) the following new paragraph:

''(5)(A) Subject to subparagraphs (B) and (C), for cost reporting periods beginning in—

''(i) fiscal year 2029, in the case of a critical access hospital that is not an essential cybersecurity practices adopter (as determined under section 1886(u)(3)(A)) for an EHR reporting period with respect to such fiscal year, the percent described in paragraph (1) shall be reduced by 0.25 percent;

''(ii) fiscal year 2030, in the case of a critical access hospital that is not an essential cybersecurity practices adopter (as determined

under section 1886(u)(3)(A)) for an EHR reporting period with respect to such fiscal year, the percent described in paragraph (1) shall be reduced by 0.50 percent;

''(iii) fiscal year 2031, in the case of a critical access hospital that is not an enhanced cybersecurity practices adopter (as determined under section 1886(u)(3)(B)) for a EHR reporting period with respect to such fiscal year, the percent described in paragraph (1) shall be reduced by 0.75 percent; and

''(iv) fiscal year 2032 or a subsequent fiscal year, in the case of a critical access hospital that is not an enhanced cybersecurity practices adopter (as determined under section 1886(u)(3)(B)) for a EHR reporting period with respect to such fiscal year, the percent described in paragraph (1) shall be reduced by 1 percent.

''(B) The percent described in paragraph (1) shall be reduced by no more than a total of 1 percent for a fiscal year as the result of the application of this paragraph and other sections of this title.

''(C) The provisions of subclause (III) of section 1886(b)(3)(B)(xiii) shall apply with respect to

subparagraph (A) for a critical access hospital with respect to a cost reporting period in the same manner as such subclause applies with respect to subclause (I) of such section for an eligible hospital.''; and

(C) in paragraph (6), as redesignated by subparagraph (A)—

(i) in subparagraph (C), by striking ''and'' at the end;

(ii) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following new subparagraphs:

''(E) the methodology and standards for determining payment amounts for critical access hospitals under section 1886(u) and payment adjustments under paragraph (5);

''(F) the methodology and standards for determining whether a critical access hospital is an essential or enhanced cybersecurity practices adopter under section 1886(u)(2) and the Secretary's determination of whether or not to apply the hardship exception under subsection (b)(3)(B)(xiii)(III) to a

critical access hospital pursuant to paragraph (5)(C); or

''(G) any alteration by the Secretary of the requirements specified in section 1886(u)(2) with respect to a critical access hospital.''.

(c) IMPLEMENTATION FUNDING.—In addition to any amounts otherwise made available, there is appropriated to the Centers for Medicare & Medicaid Services Program Management Account from the Federal Hospital Insurance Trust Fund under section 1817 of the Social Security Act (42 U.S.C. 1395i), $40,000,000 for fiscal year 2025 and $15,000,000 for each of fiscal years 2027 through 2031, to remain available until expended, to carry out the amendments made by this section.

SEC. 202. MEDICARE ACCELERATED AND ADVANCE PAYMENTS IN RESPONSE TO CYBERSECURITY INCIDENTS.

(a) PART A.—Section 1815(e)(3) of the Social Security Act (42 U.S.C. 1395g(e)(3)) is amended to read as follows:

''(3)(A) Subject to subsection (f), in the case of an eligible provider of services (as defined in subparagraph (B)) that has an agreement in effect under section 1866 and that has significant cash flow problems resulting from operations of its medicare administrative contractor under

section 1874A or from unusual circumstances of such provider's operation, including significant disruption to Medicare claims processing due to a cybersecurity incident (as defined in subparagraph (C)), the Secretary may make available appropriate accelerated payments subject to appropriate safeguards against fraud, waste, and abuse determined by the Secretary.

''(B) In this paragraph, the term 'eligible providers of services' means—

''(i) a subsection (d) hospital or a subsection (d) Puerto Rico hospital (as defined for purposes of section 1886);

''(ii) a hospital described in any of clauses (i) through (vi) of section 1886(d)(1)(B);

''(iii) a critical access hospital (as defined in section 1861(mm)(1));

''(iv) a rural emergency hospital (as defined in section 1861(kkk)(2));

''(v) a skilled nursing facility (as defined in section 1819(a));

''(vi) a home health agency (as defined in section 1861(o));

''(vii) a hospice program (as defined in section 1861(dd)(2));

''(viii) a comprehensive outpatient rehabilitation facility (as defined in section 1861(cc)(2));

''(ix) a rural health clinic (as defined in section 1861(aa)(2));

''(x) a Federally qualified health center (as defined in section 1861(aa)(4));

''(xi) an opioid treatment program (as defined in section 1861(jjj)(2)); and

''(xii) a community mental health center (as defined in section 1861(ff)(3)(B)).

''(C) In this paragraph, the term 'cybersecurity incident' has the meaning given the term 'incident' in section 2200 of the Homeland Security Act of 2002.

''(D) Notwithstanding any other provision of law, the Secretary may implement the provisions of this paragraph by program instruction or otherwise.''.

(b) PART B.—Section 1835 of the Social Security Act (42 U.S.C. 1395n) is amended by adding at the end the following new subsection:

''(f)(1) Upon the request of a supplier (as defined in section 1861(d)) that is participating in the Medicare program under this title, that is furnishing items or services under this part, and that has significant cash flow problems resulting from operations of its medicare administrative contractor under section 1874A or from unusual cir-

cumstances of such supplier's operation, including significant disruption to Medicare claims processing due to a cybersecurity incident (as defined in paragraph (2)), the Secretary may make available appropriate advance payments subject to appropriate safeguards against fraud, waste, and abuse determined by the Secretary.

''(2) In this paragraph, the term 'cybersecurity incident' has the meaning given the term 'incident' in section 2200 of the Homeland Security Act of 2002.

''(3) Notwithstanding any other provision of law, the Secretary may implement the provisions of this subsection by program instruction or otherwise.''.

(c) PROTECTION OF TRUST FUNDS.—

(1) PART A.—Section 1817 of the Social Security Act (42 U.S.C. 1395i) is amended by adding at the end the following new subsection:

''(l)(1) Beginning on the date of enactment of this subsection, there shall be transferred from the General Fund of the Treasury to the Trust Fund an amount, as estimated by the Chief Actuary of the Centers for Medicare & Medicaid Services, equal to the amount of accelerated payments made for items and services under this part.

''(2) There shall be transferred from the Trust Fund to the General Fund of the Treasury amounts equivalent to the sum of—

''(A) the amounts by which claims have offset (in whole or in part) the amount of such payments described in paragraph (1); and

''(B) the amount of such payments that have been repaid (in whole or in part).

''(3) Amounts described in paragraphs (1) and (2) shall be transferred from time to time as determined appropriate by the Secretary.''.

(2) PART B.—Section 1844 of the Social Security Act (42 U.S.C. 1395w) is amended by adding at the end the following new subsection:

''(g)(1) Beginning on the date of enactment of this subsection, there shall be transferred from the General Fund of the Treasury to the Trust Fund an amount, as estimated by the Chief Actuary of the Centers for Medicare & Medicaid Services, equal to amounts paid in advance for items and services under this part.

''(2) There shall be transferred from the Trust Fund to the General Fund of the Treasury amounts equivalent to the sum of—

''(A) the amounts by which claims have offset (in whole or in part) the amount of such payments described in paragraph (1); and

''(B) the amount of such payments that have been repaid (in whole or in part).

''(3) Amounts described in paragraphs (1) and (2) shall be transferred from time to time as determined appropriate by the Secretary.''.

○