119TH CONGRESS
1ST SESSION

S. _____

To provide additional protections with respect to health information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. CASSIDY introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To provide additional protections with respect to 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.

This Act may be cited as the ''Health Information Privacy Reform Act''.

SEC. 2. PROTECTIONS FOR APPLICABLE HEALTH INFORMATION.

(a) IN GENERAL.—The Secretary of Health and Human Services, in consultation with the Federal Trade Commission, shall promulgate regulations setting privacy,

security, and breach notifications standards for the processing of applicable health information by regulated entities and their service providers. Such standards shall provide protections that are at least commensurate with, and wherever feasible and appropriate harmonize with, the protections provided through the privacy, security, and breach notification rules promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note) and section 13402 of the HITECH Act (42 U.S.C. 17932) that apply to covered entities and business associates with respect to protected health information under such rules. Such regulations promulgated under this section shall include the following:

(1) Privacy requirements, including the following:

(A) Permitted uses and disclosures of applicable health information without an individual's written authorization that are consistent with the individual's reasonable expectations.

(B) Other permitted uses and disclosures of applicable health information without an individual's written authorization for certain public policy purposes, such as public health, health oversight, law enforcement, judicial and admin-

istrative proceedings, and any conditions for such uses and disclosures.

(C) Uses and disclosures of applicable health information that require the individual's written authorization and the requirements related to such written authorizations.

(D) Prohibited uses and disclosures of applicable health information.

(E) Minimum necessary requirements for the request, use, and disclosure of applicable health information and any exceptions.

(F) Standards and requirements related to legal representatives of the individual.

(G) Standards and requirements related to service providers.

(H) Individual rights with respect to applicable health information, including the right of the individual to receive a privacy notice from the regulated entity, access to applicable health information, amendment of applicable health information, deletion of applicable health information, and portability of applicable health information, and any exceptions to such rights (such as with respect to applicable health information collected for research purposes), any conditions

on such rights, and any other requirements related to such rights, including timeframes for responding to requests.

(I) Administrative safeguards, including designation of a privacy officer, policies and procedures, training of workforce members, non-retaliation, documentation, and mitigation.

(2) Security requirements, including the following:

(A) Physical, technical, and administrative safeguards for applicable health information in any form.

(B) For electronic applicable health information, such safeguards shall be based on well-established national frameworks, such as cybersecurity performance goals of the National Institute of Standards and Technology or the Department of Health and Human Services.

(3) Breach notification requirements in the event of a breach of applicable health information that are substantially similar to the breach notification requirements under subpart D of part 164 of title 45, Code of Federal Regulations (or any successor regulations).

(b) ENFORCEMENT AUTHORITY.—The Secretary, in consultation with the Federal Trade Commission, is authorized to enforce all provisions of this Act as described in subsection (c).

(c) CIVIL PENALTIES.—In addition to any other sanctions or remedies that may be available under any provision of Federal law, in the case of a regulated entity or service provider that violates this section, subpart D of part 160 of title 45, Code of Federal Regulations (or any successor regulations), shall apply to the regulated entity or service provider with respect to such violation of this section in the same manner that such subpart applies to a person with respect to a violation of part 160 of title 45, Code of Federal Regulations (or any successor regulations).

(d) EXTENSION OF HITECH ACT AMENDMENT TO REGULATED ENTITIES AND SERVICE PROVIDERS.—The privacy and security practices under section 13412 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17941) shall apply to regulated entities and service providers with respect to applicable health information in the same manner that such section applies to covered entities and business associates.

(e) DEFINITIONS.—In this section:

(1) APPLICABLE HEALTH INFORMATION.—The term ''applicable health information''—

(A) means information (including demographic information) that—

(i) identifies an individual or with respect to which there is a reasonable basis to believe that the information could be used to identify an individual; and

(ii) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

(B) may include information described in subparagraph (A) that was not created or received by a health care provider, health plan, employer, or health care clearinghouse.

(2) COVERED ENTITIES; BUSINESS ASSOCIATES.—The terms ''covered entities'' and ''business associates'' have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (or any successor regulations).

(3) REGULATED ENTITY.—The term ''regulated entity''—

(A) means a natural or legal person that, alone or jointly with others, determines the purpose and means of processing applicable health information; and

(B) does not include—

(i) a governmental entity such as a body, authority, board, bureau, commission, district, agency, or political subdivision of the Federal, State, or local government;

(ii) a person or an entity that is collecting, processing, or transferring covered data on behalf of or a Federal, State, Tribal, territorial, or local government entity; and

(iii) a covered entity or business associate, as such terms are defined in section 160.103 of title 45, Code of Federal Regulations (or any successor regulations).

(4) SERVICE PROVIDER.—The term ''service provider'' means a natural or legal entity that processes applicable health information on a behalf of a regulated entity and that is not a covered entity or business associate, as such terms are defined in sec-

tion 160.103 of title 45, Code of Federal Regulations (or any successor regulations).

SEC. 3. RIGHTS AND REQUIREMENTS REGARDING ACCESS TO CERTAIN PROTECTED HEALTH INFORMATION.

(a) TIME AND MANNER OF ACCESS.—In applying section 13405(e) of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17935(e)) or section 164.524(c)(3)(ii) of title 45, Code of Federal Regulations (or any successor regulations), in the case that an individual requests that a covered entity or any business associate of a covered entity transmit, produce, or provide access to a copy of the individual's protected health information to a person, including an entity, designated by the individual, and except where permitted without authorization under section 164.506(c) of title 45, Code of Federal Regulations (or any successor regulations)—

(1) the individual's request shall meet all requirements of a valid authorization under section 164.508(b) of title 45, Code of Federal Regulations (or any successor regulations); and

(2) the covered entity or business associate may condition the transmittal, production, or provision of access upon the person to whom the information is

to be transmitted or produced or to whom access is to be provided—

(A) paying fees, in accordance with applicable State law and consistent with subsection (b), in advance of such transmittal, production, or access; and

(B) acknowledging and accepting the terms, limitations, and conditions of use and disclosure contained in the request made by the individual as the legally binding obligation of the person receiving the information.

(b) FEES.—

(1) IN GENERAL.—In applying section 13405(e)(3) of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17935(e)(3)) or section 164.524(c)(4) of title 45, Code of Federal Regulations (or any successor regulations), each such section shall apply only—

(A) to the provision of access to, or the production, copying, or transmittal of, protected health information directly to—

(i) the individual, or the individual's personal representative for health care purposes as described in section 164.502(g) of

title 45, Code of Federal Regulations (or any successor regulations);

(ii) subject to paragraph (2) and section 164.510(b) of title 45, Code of Federal Regulations (or any successor regulation), any other person identified in, and subject to the limitations of, such section; or

(iii) the individual's health care provider or the business associates of such provider; and

(B) as directed by the individual, to the electronic transmittal of the individual's electronic health record to the patient portal or mobile medical application used and maintained by the individual's health care provider or for the health care provider by its business associate.

(2) ADDITIONAL LIMITATIONS.—In the case of the provision of access to, or the production, copying, or transmittal of, protected health information under paragraph (1)(A) directly to a person described in clause (ii) of such paragraph, such protected health information shall, in accordance with section 164.510(b) of title 45, Code of Federal Reg-

ulations (or any successor regulations), be limited to only such information that is—

(A) directly relevant to the person's involvement with the care of the individual or with the payment relevant to the care of the individual; or

(B) needed for notification purposes described in such section.

(c) DEFINITIONS.—In this section, the terms ''business associate'', ''covered entity'', ''health care provider'', ''individual'', ''person'', and ''protected health information'' have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (or any successor regulations).

(d) GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Secretary of Health and Human Services shall amend existing guidance as necessary to implement subsections (a) and (b).

SEC. 4. CONFIDENTIALITY OF RECORDS.

Section 543 of the Public Health Service Act (42 U.S.C. 290dd–2) is amended—

(1) in subsection (a), by striking ''subsection (b)'' and inserting ''the HIPAA regulations'';

(2) in subsection (b)—

(A) in paragraph (2), by redesignating subparagraphs (A) through (D) as paragraphs (1) through (4), respectively, and adjusting the margins accordingly; and

(B) by striking ''(b) PERMITTED DISCLOSURE'' and all that follows through ''(2) METHOD FOR DISCLOSURE—Whether'' and inserting the following:

''(b) PERMITTED DISCLOSURE.—Whether'';

(3) in subsection (c), in the matter preceding paragraph (1), by striking ''subsection (b)(2)(C)'' and inserting ''subsection (b)(3)''; and

(4) in subsection (g), by striking ''subsection (b)(2)(C)'' and inserting ''subsection (b)(3)''.

SEC. 5. NAS STUDY ON COMPENSATION TO PATIENTS FOR SHARING IDENTIFIABLE DATA FOR RESEARCH PURPOSES.

(a) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary of Health and Human Services shall seek to enter into a contract with the National Academies of Sciences, Engineering, and Medicine to conduct a study examining potential risks and benefits of paying compensation to patients for sharing their identifiable data for research purposes.

(b) INCLUSIONS.—The study conducted pursuant to the contract under subsection (a) shall include an examination of—

(1) the risks to patient privacy posed by the integration of identifiable, de-identified, and aggregated health information into datasets used for research;

(2) privacy enhancing tools and methods for the protection of patient health data;

(3) the feasibility of tracking patient data and consent for the integration of patient health data into datasets used for research;

(4) ethical considerations for compensating patients for use of their identifiable and de-identified health data;

(5) whether the existing exemptions permitting de-identified data to be used for research should consider whether a patient was given an opportunity to opt-in or opt-out of participation; and

(6) risk of re-identification of de-identified data.

SEC. 6. PATIENT NOTIFICATION REQUIREMENTS UNDER THE HIPAA PRIVACY REGULATIONS.

(a) PATIENT NOTIFICATION UPON REMOVAL.—Any regulated entity or service provider who gains access to the protected health information of an individual through

the patient right of access under section 164.524 of title 45, Code of Federal Regulations (or any successor regulations) shall—

(1) provide a written plain language notification to such individual prior to accessing such information—

(A) that such protected health information will no longer be subject to the protections under the HIPAA privacy regulation; and

(B) that includes an explanation of how and to which entities such protected health information may be redisclosed; and

(2) require the consent of the individual before selling such protected health information to third parties.

(b) PATIENT NOTIFICATION REGARDING WELLNESS DATA.—

(1) IN GENERAL.—Any regulated entity or service provider who offers digital technology that generates wellness data about individuals shall, with respect to each individual who uses such technology—

(A) provide a written plain language notification to the individual in advance of initiating the generation of such data that such data will

not be subject to the protections of the HIPAA privacy regulation; and

(B) offer the individual an opportunity to opt out of such wellness data generation.

(2) WELLNESS DATA.—In this subsection, the term ''wellness data'' means data generated for the purpose of promoting health or preventing disease, which may include vital statistics, step counts, and medical regimen compliance.

(c) DEFINITIONS.—In this section—

(1) the terms ''business associate'', ''covered entity'', and ''protected health information'' have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (or any successor regulations));

(2) the term ''HIPAA privacy regulation'' has the meaning given such term in section 1180(b)(3) of the Social Security Act (42 U.S.C. 1320d–9(b)(3)); and

(3) the terms ''regulated entity'' and ''service provider'' have the meanings given such terms in section 2.

(d) EFFECTIVE DATE.—This section shall take effect beginning one year after the date of enactment of this Act.

SEC. 7. MINIMUM NECESSARY GUIDANCE.

Not later than 1 year after the date of enactment of this Act, the Secretary of Health and Human Services shall publish guidance on the application of the minimum necessary standard to data used for artificial intelligence and other machine learning applications and relevant requirements, including health data interoperability requirements under section 3001(c)(9) of the Public Health Service Act (42 U.S.C. 300jj–11(c)(9)) and the use of limited data sets pursuant to section 13405(b) of the HITECH Act (42 U.S.C. 17935(b)).

SEC. 8. DE-IDENTIFIED INFORMATION.

(a) ESTABLISHMENT OF STANDARDS.—Not later than 1 year after the date of enactment of this Act, the Secretary of Health and Human Services shall promulgate regulations establishing unified national standards for rendering applicable health information as de-identified information, in a manner similar to the manner in which individually identifiable health information may be rendered de-identified information pursuant to part 164 of title 45, Code of Federal Regulations (or any successor regulations).

(b) COMPOSITION OF STANDARDS.—Such standards shall—

(1) be at least equivalent to or exceed the de-identification standard specified in section

164.514(b) of title 45, Code of Federal Regulations (or any successor regulations);

(2) specify standards for the use of privacy-enhancing technologies as a method for creating de-identified information; and

(3) specify that information shall not qualify as de-identified information when provided by a regulated entity, service provider, covered entity, or business associate to another person or entity unless such person or entity contractually agrees in writing not to re-identify or attempt to re-identify the information, and to require the same of any person or entity to whom such person or entity provides the information.

(c) DEFINITIONS.—In this section—

(1) the term ''applicable health information'' has the meaning given such term in section 2;

(2) the terms ''business associate'', ''covered entity'', and ''individually identifiable health information'' have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (or any successor regulations); and

(3) the term ''privacy enhancing technologies'' means any software or hardware solution, technical process, or other technological means of mitigating

individuals' privacy risks arising from data processing by enhancing predictability, manageability, disassociability, and confidentiality.

SEC. 9. PREEMPTION.

Section 160.203 of title 45, Code of Federal Regulations (or any successor regulations) shall apply to the requirements set forth under this Act in the same manner and to the same extent as such section applies to the standards, requirements, and implementation specifications under subchapter C of chapter I of subtitle A of title 45, Code of Federal Regulations (or any successor regulations).