TAM26851 CNH

Bill Cassidy M.D.

S.L.C.

AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—119th Cong., 2d Sess.

S. 3097

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

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by _____

Viz:

Strike all after the enacting clause and insert the following:

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.—Not later than 18 months after the date of enactment of this Act, the Secretary of Health and Human Services (referred to in this section as the "Secretary"), in consultation with the Federal Trade Commission, shall promulgate regulations establishing and

implementing privacy, security, and breach notification standards for the processing of applicable health information by regulated entities and their service providers. Such standards shall provide rights and protections that are at least equivalent to, and that, wherever feasible and appropriate, harmonize with, the rights and 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, taking into consideration the context in which the applicable health information was obtained, provided that such regulations shall not authorize such a use or disclosure to investigate, or to impose liability on, any individual in connection

with the seeking, obtaining, providing, or facilitating of health care.

(B) Uses and disclosures of applicable health information that require the individual's written authorization and the requirements related to such written authorizations, including how the individual may revoke such authorization, which shall include requiring the individual's written authorization for any sale, license, transfer, or marketing of applicable health information.

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

(D) Minimum necessary requirements for the request, use, and disclosure of applicable health information and any exceptions that are necessary for purpose specification, collection limitation, data minimization, and limitation on secondary use and consistent with subsection (b).

(E) Standards and requirements for an individual to be authorized to exercise the rights granted in this section with respect to applicable health information of another individual.

(F) Standards and requirements related to service providers.

(G)(i) Individual rights with respect to applicable health information, including the following:

(I) The right of the individual to receive a privacy notice from the regulated entity, which shall describe the purposes for which the regulated entity uses and discloses applicable health information, the rights of the individual under this subparagraph, and the manner in which such rights may be exercised.

(II) The right of access to applicable health information, including the ability of the individual to direct the transmission of applicable health information held in an electronic health record to a third party.

(III) The right to amendment of applicable health information.

(IV) The right to deletion of applicable health information, not later than 30 days after the regulated entity or service provider receives a request for such a deletion, and allowing for the regulated entity

or service provider to communicate with the individual making such request prior to fulfilling such request.

(V) The right to portability of applicable health information, including the ability of the individual to transfer such information between applications, services, or devices.

(ii) Any exception to, or condition or other requirement on, a right described in any of subclauses (I) through (V) of clause (i), including an exception with respect to applicable health information collected for research purposes and a timeframe for responding to a request of an individual for applicable health information.

(H) 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 written or oral form.

(B) The application of the standards under subpart C of part 164 of title 45, Code of Federal Regulations (or any successor regulations) to electronic applicable health information in the same manner as such standards apply to electronic protected health information.

(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) for applicable health information that is not subject to the health breach notification rule at part 318 of title 16, Code of Federal Regulations (or any successor regulations).

(b) REQUIREMENTS FOR REGULATED ENTITIES AND SERVICE PROVIDERS.—

(1) DATA MINIMIZATION.—A regulated entity or service provider may not collect, process, or transfer applicable health information beyond what a covered entity is permitted to collect, process, or transfer under sections 164.502(b) and 164.514(d) of title 45, Code of Federal Regulations (or any successor regulations).

(2) RETENTION.—A regulated entity or service provider may not retain applicable health information for longer than is reasonably necessary to carry out the purpose for which such information was collected.

(3) EXCEPTIONS.—Paragraphs (1) and (2) shall not apply to the collection, processing, or transfer of applicable health information to the extent reasonably necessary for any of the following purposes:

(A) To complete a transaction or provide a product or service specifically requested by the individual to whom such information relates.

(B) To comply with a legal obligation, or to establish, exercise, or defend a legal claim.

(C) To prevent, detect, or respond to a security incident, fraud, or harm to an individual.

(D) To carry out a public health activity permitted under the regulations promulgated under subsection (a).

(E) To conduct research subject to part 46 of title 45, Code of Federal Regulations, or part 50 or 56 of title 21, Code of Federal Regulations (or any successor regulations).

(c) ENFORCEMENT.—

(1) COORDINATION.—Not later than 180 days after the date of enactment of this Act, the Secretary and the Federal Trade Commission shall enter into a memorandum of understanding that allocates primary enforcement responsibility under this section, provides for mutual notification of investigations into violations of this section, and ensures that a regulated entity or service provider is not subject to duplicative civil penalties for the same act or omission.

(2) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to limit or supersede the authority of the Federal Trade Commission under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(3) 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, 162, or 164 of

subchapter C of chapter I of subtitle A of title 45, Code of Federal Regulations (or any successor regulations). Any funds collected through civil penalties under this paragraph shall be used to support enforcement activity under this section.

(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. Not later than 18 months after the date of enactment of this Act, the Secretary shall promulgate regulations to carry out this subsection.

(e) GOVERNMENT ACCESS.—A regulated entity or service provider may not sell or otherwise transfer applicable health information to a Federal, State, local, Tribal, or territorial governmental entity except as compelled by warrant, subpoena, court order, or other compulsory process.

(f) DEFINITIONS.—In this section:

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

(A) means information (including demographic information)—

(i) that 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) that relates to the past, present, or future physical or mental health or condition of such individual, the past, present, or future provision of health care to such individual, or past, present, or future payment for the provision of health care to such individual;

(B) includes—

(i) information described in subparagraph (A) that was not created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(ii) precise geolocation information that could reasonably indicate an attempt by an individual to acquire or receive a health service or supply; and

(C) does not include—

(i) information subject to—

(I) title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

(II) the requirements regarding the confidentiality of substance use disorder information under section 543 of the Public Health Service Act (42 U.S.C. 290dd–2);

(III) section 444 of the General Education Provisions Act (20 U.S.C. 1232g; commonly known as the "Family Educational Rights and Privacy Act of 1974") and part 99 of title 34, Code of Federal Regulations (or any successor regulations) to the extent such regulated entity or service provider is an educational agency or institution as defined in such section of such Act or section 99.3 of title 34, Code of Federal Regulations (or any successor regulations);

(IV) provisions for the protection of identifiable private information that is collected pursuant to—

(aa) the Federal requirements for the protection of

human subjects under part 46 of title 45, Code of Federal Regulations or part 50 or 56 of title 21, Code of Federal Regulations (or any successor regulations); or

(bb) the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(V) the Health Care Quality Improvement Act of 1986 (42 U.S.C. 11101 et seq.); or

(VI) part C of title IX of the Public Health Service Act (42 U.S.C. 299b–21 et seq.);

(ii) publicly available information; or

(iii) information collected, processed, or transferred by an individual in the course of a purely personal or household activity.

(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) DATA BROKER.—The term "data broker" means a regulated entity whose principal source of revenue is derived from processing or transferring applicable health information that the entity did not collect directly from the individuals to whom such information relates.

(4) 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, including a data broker; and

(B) does not include—

(i) a covered entity or business associate, with respect to protected health information; or

(ii) an individual who is the subject of the applicable health information or who obtains applicable health information in a personal or household capacity.

(5) SERVICE PROVIDER.—The term "service provider" means a natural or legal entity that processes applicable health information on behalf of a

regulated entity and that is not a covered entity or business associate.

(g) REGULATIONS.—The Secretary may promulgate regulations to carry out this section.

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 in an electronic health record to a person designated by the individual, 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—

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

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

(1) the individual, or the individual's personal representative;

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

(3) a personal health record managed and controlled by the individual.

(c) DEFINITIONS.—In this section—

(1) 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); and

(2) the term "personal health record" has the meaning given such term in section 13400 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921).

(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).

(e) RULES OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) permit a covered entity or business associate to deny, delay, or condition a transmission directed by an individual in a manner that constitutes information blocking under section 3022 of the Public Health Service Act (42 U.S.C. 300jj–52) or part 171 of title 45, Code of Federal Regulations (or any successor regulations);

(2) treat an individual or the individual's personal representative who receives or accesses the individual's protected health information on the individual's behalf and at the direction of the individual as a person to whom a fee or condition may be applied under subsection (a), with respect to a personal health record that is selected, managed, and con-

trolled by the individual or the individual's personal representative; or

(3) alter the rights or responsibilities of covered entities and individuals under section 13405(e) of the HITECH Act (42 U.S.C. 17935).

SEC. 4. MINIMUM NECESSARY GUIDANCE.

(a) RULEMAKING.—Not later than 1 year after the date of enactment of this Act, the Secretary of Health and Human Services (referred to in this section as the "Secretary"), in coordination with the Commissioner of Food and Drugs and the National Coordinator for Health Information Technology, shall promulgate regulations regarding the application of the minimum necessary standard under section 164.502(b) of title 45, Code of Federal Regulations, to applicable health information and protected health information, including such information used to train, develop, validate, modify, or operate an artificial intelligence or other machine learning model.

(b) CONTENTS.—The regulations promulgated under subsection (a) shall—

(1) clarify that such minimum necessary standard does not permit a covered entity, business associate, regulated entity, or service provider to deny, delay, or condition a use or disclosure that is otherwise required or permitted, including a disclosure re-

quired under section 3022 of the Public Health Service Act (42 U.S.C. 300jj–52), on the ground that limiting the disclosure to the minimum necessary information is not technically feasible, and, as applicable, the minimum necessary standard is satisfied by reasonable efforts to limit the information used or disclosed, even where further technical limitation is not feasible;

(2) specify how the minimum necessary standard applies to the use of applicable health information and protected health information to develop, train, validate, or fine-tune an artificial intelligence or machine learning model, including the circumstances under which the use of a larger data set is reasonably necessary for such development and the extent to which de-identification, data minimization, or privacy enhancing technologies satisfy the standard; and

(3) address the minimum necessary standard with respect to the health data interoperability requirements under sections 3001(c)(9) and 3022 of the Public Health Service Act (42 U.S.C. 300jj–11(c)(9), 300jj–52) and part 171 of title 45, Code of Federal Regulations (or any successor regulations).

(c) PERIODIC REVIEW.—The Secretary shall review, and update as appropriate, the regulations promulgated under subsection (a) not less frequently than once every 3 years.

SEC. 5. 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.—The standards under subsection (a) shall—

(1) be at least as protective as the de-identification standard specified in section 164.514(b)(1) of title 45, Code of Federal Regulations (or any successor regulations) (relating to expert determination), and may not permit information to be rendered de-identified information solely through the method specified in section 164.514(b)(2) of such title (relating to safe harbor);

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

(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; and

(4) account for evolving methods of re-identification, including methods that use artificial intelligence or machine learning.

(c) PROHIBITION ON RE-IDENTIFICATION.—An entity that is the recipient of de-identified information may not re-identify, or attempt to re-identify, such information. A violation of this subsection shall be enforceable and subject to the civil penalties under section 2(c).

(d) 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 informa-

tion'' 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. 6. 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).