

Bill Cassidy M.D.

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:

1 Strike all after the enacting clause and insert the fol-
2 lowing:3 **SECTION 1. SHORT TITLE.**4 This Act may be cited as the "Health Information
5 Privacy Reform Act".6 **SEC. 2. PROTECTIONS FOR APPLICABLE HEALTH INFORMA-**
7 **TION.**8 (a) IN GENERAL.—Not later than 18 months after
9 the date of enactment of this Act, the Secretary of Health
10 and Human Services (referred to in this section as the
11 "Secretary"), in consultation with the Federal Trade
12 Commission, shall promulgate regulations establishing and

1 implementing privacy, security, and breach notification
2 standards for the processing of applicable health informa-
3 tion by regulated entities and their service providers. Such
4 standards shall provide rights and protections that are at
5 least equivalent to, and that, wherever feasible and appro-
6 priate, harmonize with, the rights and protections pro-
7 vided through the privacy, security, and breach notifica-
8 tion rules promulgated under section 264(e) of the Health
9 Insurance Portability and Accountability Act of 1996 (42
10 U.S.C. 1320d–2 note) and section 13402 of the HITECH
11 Act (42 U.S.C. 17932) that apply to covered entities and
12 business associates with respect to protected health infor-
13 mation under such rules. Such regulations promulgated
14 under this section shall include the following:

15 (1) Privacy requirements, including the fol-
16 lowing:

17 (A) Permitted uses and disclosures of ap-
18 plicable health information without an individ-
19 ual's written authorization that are consistent
20 with the individual's reasonable expectations,
21 taking into consideration the context in which
22 the applicable health information was obtained,
23 provided that such regulations shall not author-
24 ize such a use or disclosure to investigate, or to
25 impose liability on, any individual in connection

1 with the seeking, obtaining, providing, or facili-
2 tating of health care.

3 (B) Uses and disclosures of applicable
4 health information that require the individual's
5 written authorization and the requirements re-
6 lated to such written authorizations, including
7 how the individual may revoke such authoriza-
8 tion, which shall include requiring the individ-
9 ual's written authorization for any sale, license,
10 transfer, or marketing of applicable health in-
11 formation.

12 (C) Prohibited uses and disclosures of ap-
13 plicable health information.

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

21 (E) Standards and requirements for an in-
22 dividual to be authorized to exercise the rights
23 granted in this section with respect to applica-
24 ble health information of another individual.

1 (F) Standards and requirements related to
2 service providers.

3 (G)(i) Individual rights with respect to ap-
4 plicable health information, including the fol-
5 lowing:

6 (I) The right of the individual to re-
7 ceive a privacy notice from the regulated
8 entity, which shall describe the purposes
9 for which the regulated entity uses and
10 discloses applicable health information, the
11 rights of the individual under this subpara-
12 graph, and the manner in which such
13 rights may be exercised.

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

19 (III) The right to amendment of ap-
20 plicable health information.

21 (IV) The right to deletion of applica-
22 ble health information, not later than 30
23 days after the regulated entity or service
24 provider receives a request for such a dele-
25 tion, and allowing for the regulated entity

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

4 (V) The right to portability of applica-
5 ble health information, including the ability
6 of the individual to transfer such informa-
7 tion between applications, services, or de-
8 vices.

9 (ii) Any exception to, or condition or other
10 requirement on, a right described in any of sub-
11 clauses (I) through (V) of clause (i), including
12 an exception with respect to applicable health
13 information collected for research purposes and
14 a timeframe for responding to a request of an
15 individual for applicable health information.

16 (H) Administrative safeguards, including
17 designation of a privacy officer, policies and
18 procedures, training of workforce members,
19 non-retaliation, documentation, and mitigation.

20 (2) Security requirements, including the fol-
21 lowing:

22 (A) Physical, technical, and administrative
23 safeguards for applicable health information in
24 written or oral form.

1 (B) The application of the standards under
2 subpart C of part 164 of title 45, Code of Fed-
3 eral Regulations (or any successor regulations)
4 to electronic applicable health information in
5 the same manner as such standards apply to
6 electronic protected health information.

7 (3) Breach notification requirements in the
8 event of a breach of applicable health information
9 that are substantially similar to the breach notifica-
10 tion requirements under subpart D of part 164 of
11 title 45, Code of Federal Regulations (or any suc-
12 cessor regulations) for applicable health information
13 that is not subject to the health breach notification
14 rule at part 318 of title 16, Code of Federal Regula-
15 tions (or any successor regulations).

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

18 (1) DATA MINIMIZATION.—A regulated entity
19 or service provider may not collect, process, or trans-
20 fer applicable health information beyond what a cov-
21 ered entity is permitted to collect, process, or trans-
22 fer under sections 164.502(b) and 164.514(d) of
23 title 45, Code of Federal Regulations (or any suc-
24 cessor regulations).

1 (2) RETENTION.—A regulated entity or service
2 provider may not retain applicable health informa-
3 tion for longer than is reasonably necessary to carry
4 out the purpose for which such information was col-
5 lected.

6 (3) EXCEPTIONS.—Paragraphs (1) and (2)
7 shall not apply to the collection, processing, or trans-
8 fer of applicable health information to the extent
9 reasonably necessary for any of the following pur-
10 poses:

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

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

16 (C) To prevent, detect, or respond to a se-
17 curity incident, fraud, or harm to an individual.

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

21 (E) To conduct research subject to part 46
22 of title 45, Code of Federal Regulations, or part
23 50 or 56 of title 21, Code of Federal Regula-
24 tions (or any successor regulations).

25 (c) ENFORCEMENT.—

1 (1) COORDINATION.—Not later than 180 days
2 after the date of enactment of this Act, the Sec-
3 retary and the Federal Trade Commission shall
4 enter into a memorandum of understanding that al-
5 locates primary enforcement responsibility under this
6 section, provides for mutual notification of investiga-
7 tions into violations of this section, and ensures that
8 a regulated entity or service provider is not subject
9 to duplicative civil penalties for the same act or
10 omission.

11 (2) RULE OF CONSTRUCTION.—Nothing in this
12 Act shall be construed to limit or supersede the au-
13 thority of the Federal Trade Commission under sec-
14 tion 5 of the Federal Trade Commission Act (15
15 U.S.C. 45).

16 (3) CIVIL PENALTIES.—In addition to any other
17 sanctions or remedies that may be available under
18 any provision of Federal law, in the case of a regu-
19 lated entity or service provider that violates this sec-
20 tion, subpart D of part 160 of title 45, Code of Fed-
21 eral Regulations (or any successor regulations) shall
22 apply to the regulated entity or service provider with
23 respect to such violation of this section in the same
24 manner that such subpart applies to a person with
25 respect to a violation of part 160, 162, or 164 of

1 subchapter C of chapter I of subtitle A of title 45,
2 Code of Federal Regulations (or any successor regu-
3 lations). Any funds collected through civil penalties
4 under this paragraph shall be used to support en-
5 forcement activity under this section.

6 (d) EXTENSION OF HITECH ACT AMENDMENT TO
7 REGULATED ENTITIES AND SERVICE PROVIDERS.—The
8 privacy and security practices under section 13412 of the
9 Health Information Technology for Economic and Clinical
10 Health Act (42 U.S.C. 17941) shall apply to regulated en-
11 tities and service providers with respect to applicable
12 health information in the same manner that such section
13 applies to covered entities and business associates. Not
14 later than 18 months after the date of enactment of this
15 Act, the Secretary shall promulgate regulations to carry
16 out this subsection.

17 (e) GOVERNMENT ACCESS.—A regulated entity or
18 service provider may not sell or otherwise transfer applica-
19 ble health information to a Federal, State, local, Tribal,
20 or territorial governmental entity except as compelled by
21 warrant, subpoena, court order, or other compulsory proce-
22 ss.

23 (f) DEFINITIONS.—In this section:

24 (1) APPLICABLE HEALTH INFORMATION.—The
25 term “applicable health information”—

10

1 (A) means information (including demo-
2 graphic information)—

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

7 (ii) that relates to the past, present,
8 or future physical or mental health or con-
9 dition of such individual, the past, present,
10 or future provision of health care to such
11 individual, or past, present, or future pay-
12 ment for the provision of health care to
13 such individual;

14 (B) includes—

15 (i) information described in subpara-
16 graph (A) that was not created or received
17 by a health care provider, health plan, em-
18 ployer, or health care clearinghouse; and

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

23 (C) does not include—

24 (i) information subject to—

11

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

3 (II) the requirements regarding
4 the confidentiality of substance use
5 disorder information under section
6 543 of the Public Health Service Act
7 (42 U.S.C. 290dd-2);

8 (III) section 444 of the General
9 Education Provisions Act (20 U.S.C.
10 1232g; commonly known as the
11 “Family Educational Rights and Pri-
12 vacy Act of 1974”) and part 99 of
13 title 34, Code of Federal Regulations
14 (or any successor regulations) to the
15 extent such regulated entity or service
16 provider is an educational agency or
17 institution as defined in such section
18 of such Act or section 99.3 of title 34,
19 Code of Federal Regulations (or any
20 successor regulations);

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

24 (aa) the Federal require-
25 ments for the protection of

1 human subjects under part 46 of
2 title 45, Code of Federal Regula-
3 tions or part 50 or 56 of title 21,
4 Code of Federal Regulations (or
5 any successor regulations); or

6 (bb) the good clinical prac-
7 tice guidelines issued by the
8 International Council for
9 Harmonisation of Technical Re-
10 quirements for Pharmaceuticals
11 for Human Use;

12 (V) the Health Care Quality Im-
13 provement Act of 1986 (42 U.S.C.
14 11101 et seq.); or

15 (VI) part C of title IX of the
16 Public Health Service Act (42 U.S.C.
17 299b-21 et seq.);

18 (ii) publicly available information; or

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

23 (2) COVERED ENTITIES; BUSINESS ASSOCI-
24 ATES.—The terms “covered entities” and “business
25 associates” have the meanings given such terms in

1 section 160.103 of title 45, Code of Federal Regula-
2 tions (or any successor regulations).

3 (3) DATA BROKER.—The term “data broker”
4 means a regulated entity whose principal source of
5 revenue is derived from processing or transferring
6 applicable health information that the entity did not
7 collect directly from the individuals to whom such in-
8 formation relates.

9 (4) REGULATED ENTITY.—The term “regulated
10 entity”—

11 (A) means a natural or legal person that,
12 alone or jointly with others, determines the pur-
13 pose and means of processing applicable health
14 information, including a data broker; and

15 (B) does not include—

16 (i) a covered entity or business asso-
17 ciate, with respect to protected health in-
18 formation; or

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

23 (5) SERVICE PROVIDER.—The term “service
24 provider” means a natural or legal entity that proc-
25 esses applicable health information on behalf of a

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

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

5 **SEC. 3. RIGHTS AND REQUIREMENTS REGARDING ACCESS**
6 **TO CERTAIN PROTECTED HEALTH INFORMA-**
7 **TION.**

8 (a) TIME AND MANNER OF ACCESS.—In applying
9 section 13405(e) of the Health Information Technology
10 for Economic and Clinical Health Act (42 U.S.C.
11 17935(e)) or section 164.524(c)(3)(ii) of title 45, Code of
12 Federal Regulations (or any successor regulations), in the
13 case that an individual requests that a covered entity or
14 any business associate of a covered entity transmit,
15 produce, or provide access to a copy of the individual's
16 protected health information in an electronic health record
17 to a person designated by the individual, the covered entity
18 or business associate may condition the transmittal, pro-
19 duction, or provision of access upon the person to whom
20 the information is to be transmitted or produced or to
21 whom access is to be provided—

22 (1) paying fees, in accordance with applicable
23 State law and consistent with subsection (b), in ad-
24 vance of such transmittal, production, or access; and

1 (2) acknowledging and accepting the terms, lim-
2 itations, and conditions of use and disclosure con-
3 tained in the request made by the individual as the
4 legally binding obligation of the person receiving the
5 information.

6 (b) FEES.—In applying section 13405(e)(3) of the
7 Health Information Technology for Economic and Clinical
8 Health Act (42 U.S.C. 17935(e)(3)) or section
9 164.524(e)(4) of title 45, Code of Federal Regulations (or
10 any successor regulations), each such section shall apply
11 only to the provision of access to, or the production, copy-
12 ing, or transmittal of, protected health information to—

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

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

17 (3) a personal health record managed and con-
18 trolled by the individual.

19 (c) DEFINITIONS.—In this section—

20 (1) the terms “business associate”, “covered en-
21 tity”, “health care provider”, “individual”, “per-
22 son”, and “protected health information” have the
23 meanings given such terms in section 160.103 of
24 title 45, Code of Federal Regulations (or any suc-
25 cessor regulations); and

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

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

9 (e) RULES OF CONSTRUCTION.—Nothing in this sec-
10 tion shall be construed to—

11 (1) permit a covered entity or business asso-
12 ciate to deny, delay, or condition a transmission di-
13 rected by an individual in a manner that constitutes
14 information blocking under section 3022 of the Pub-
15 lic Health Service Act (42 U.S.C. 300jj–52) or part
16 171 of title 45, Code of Federal Regulations (or any
17 successor regulations);

18 (2) treat an individual or the individual’s per-
19 sonal representative who receives or accesses the in-
20 dividual’s protected health information on the indi-
21 vidual’s behalf and at the direction of the individual
22 as a person to whom a fee or condition may be ap-
23 plied under subsection (a), with respect to a personal
24 health record that is selected, managed, and con-

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

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

6 **SEC. 4. MINIMUM NECESSARY GUIDANCE.**

7 (a) RULEMAKING.—Not later than 1 year after the
8 date of enactment of this Act, the Secretary of Health and
9 Human Services (referred to in this section as the “Sec-
10 retary”), in coordination with the Commissioner of Food
11 and Drugs and the National Coordinator for Health Infor-
12 mation Technology, shall promulgate regulations regard-
13 ing the application of the minimum necessary standard
14 under section 164.502(b) of title 45, Code of Federal Reg-
15 ulations, to applicable health information and protected
16 health information, including such information used to
17 train, develop, validate, modify, or operate an artificial in-
18 telligence or other machine learning model.

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

21 (1) clarify that such minimum necessary stand-
22 ard does not permit a covered entity, business asso-
23 ciate, regulated entity, or service provider to deny,
24 delay, or condition a use or disclosure that is other-
25 wise required or permitted, including a disclosure re-

1 quired under section 3022 of the Public Health
2 Service Act (42 U.S.C. 300jj–52), on the ground
3 that limiting the disclosure to the minimum nec-
4 essary information is not technically feasible, and, as
5 applicable, the minimum necessary standard is satis-
6 fied by reasonable efforts to limit the information
7 used or disclosed, even where further technical limi-
8 tation is not feasible;

9 (2) specify how the minimum necessary stand-
10 ard applies to the use of applicable health informa-
11 tion and protected health information to develop,
12 train, validate, or fine-tune an artificial intelligence
13 or machine learning model, including the cir-
14 cumstances under which the use of a larger data set
15 is reasonably necessary for such development and
16 the extent to which de-identification, data minimiza-
17 tion, or privacy enhancing technologies satisfy the
18 standard; and

19 (3) address the minimum necessary standard
20 with respect to the health data interoperability re-
21 quirements under sections 3001(c)(9) and 3022 of
22 the Public Health Service Act (42 U.S.C. 300jj–
23 11(c)(9), 300jj–52) and part 171 of title 45, Code
24 of Federal Regulations (or any successor regula-
25 tions).

1 (c) PERIODIC REVIEW.—The Secretary shall review,
2 and update as appropriate, the regulations promulgated
3 under subsection (a) not less frequently than once every
4 3 years.

5 **SEC. 5. DE-IDENTIFIED INFORMATION.**

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

16 (b) COMPOSITION OF STANDARDS.—The standards
17 under subsection (a) shall—

18 (1) be at least as protective as the de-identifica-
19 tion standard specified in section 164.514(b)(1) of
20 title 45, Code of Federal Regulations (or any suc-
21 cessor regulations) (relating to expert determina-
22 tion), and may not permit information to be ren-
23 dered de-identified information solely through the
24 method specified in section 164.514(b)(2) of such
25 title (relating to safe harbor);

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

4 (3) specify that information shall not qualify as
5 de-identified information when provided by a regu-
6 lated entity, service provider, covered entity, or busi-
7 ness associate to another person or entity unless
8 such person or entity contractually agrees in writing
9 not to re-identify or attempt to re-identify the infor-
10 mation, and to require the same of any person or en-
11 tity to whom such person or entity provides the in-
12 formation; and

13 (4) account for evolving methods of re-identi-
14 fication, including methods that use artificial intel-
15 ligence or machine learning.

16 (c) PROHIBITION ON RE-IDENTIFICATION.—An enti-
17 ty that is the recipient of de-identified information may
18 not re-identify, or attempt to re-identify, such information.
19 A violation of this subsection shall be enforceable and sub-
20 ject to the civil penalties under section 2(c).

21 (d) DEFINITIONS.—In this section—

22 (1) the term “applicable health information”
23 has the meaning given such term in section 2;

24 (2) the terms “business associate”, “covered en-
25 tity”, and “individually identifiable health informa-

1 tion” have the meanings given such terms in section
2 160.103 of title 45, Code of Federal Regulations (or
3 any successor regulations); and

4 (3) the term “privacy enhancing technologies”
5 means any software or hardware solution, technical
6 process, or other technological means of mitigating
7 individuals’ privacy risks arising from data proc-
8 essing by enhancing predictability, manageability,
9 disassociability, and confidentiality.

10 **SEC. 6. PREEMPTION.**

11 Section 160.203 of title 45, Code of Federal Regula-
12 tions (or any successor regulations) shall apply to the re-
13 quirements set forth under this Act in the same manner
14 and to the same extent as such section applies to the
15 standards, requirements, and implementation specifica-
16 tions under subchapter C of chapter I of subtitle A of title
17 45, Code of Federal Regulations (or any successor regula-
18 tions).