

119TH CONGRESS
1ST SESSION

S. 3097

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

IN THE SENATE OF THE UNITED STATES

NOVEMBER 4, 2025

Mr. CASSIDY introduced the following bill; which was read twice and referred
to the Committee on Health, Education, Labor, and Pensions

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

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.—The Secretary of Health and
9 Human Services, in consultation with the Federal Trade
10 Commission, shall promulgate regulations setting privacy,

1 security, and breach notifications standards for the proc-
2 essing of applicable health information by regulated enti-
3 ties and their service providers. Such standards shall pro-
4 vide protections that are at least commensurate with, and
5 wherever feasible and appropriate harmonize with, the
6 protections provided through the privacy, security, and
7 breach notification rules promulgated under section 264(c)
8 of the Health Insurance Portability and Accountability
9 Act of 1996 (42 U.S.C. 1320d–2 note) and section 13402
10 of the HITECH Act (42 U.S.C. 17932) that apply to cov-
11 ered entities and business associates with respect to pro-
12 tected health information under such rules. Such regula-
13 tions promulgated under this section shall include the fol-
14 lowing:

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 (B) Other permitted uses and disclosures
22 of applicable health information without an in-
23 dividual’s written authorization for certain pub-
24 lic policy purposes, such as public health, health
25 oversight, law enforcement, judicial and admin-

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

3 (C) 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.

7 (D) Prohibited uses and disclosures of ap-
8 plicable health information.

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

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

14 (G) Standards and requirements related to
15 service providers.

16 (H) Individual rights with respect to appli-
17 cable health information, including the right of
18 the individual to receive a privacy notice from
19 the regulated entity, access to applicable health
20 information, amendment of applicable health in-
21 formation, deletion of applicable health informa-
22 tion, and portability of applicable health infor-
23 mation, and any exceptions to such rights (such
24 as with respect to applicable health information
25 collected for research purposes), any conditions

1 on such rights, and any other requirements re-
2 lated to such rights, including timeframes for
3 responding to requests.

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

8 (2) Security requirements, including the fol-
9 lowing:

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

13 (B) For electronic applicable health infor-
14 mation, such safeguards shall be based on well-
15 established national frameworks, such as cyber-
16 security performance goals of the National In-
17 stitute of Standards and Technology or the De-
18 partment of Health and Human Services.

19 (3) Breach notification requirements in the
20 event of a breach of applicable health information
21 that are substantially similar to the breach notifica-
22 tion requirements under subpart D of part 164 of
23 title 45, Code of Federal Regulations (or any suc-
24 cessor regulations).

1 (b) ENFORCEMENT AUTHORITY.—The Secretary, in
2 consultation with the Federal Trade Commission, is au-
3 thorized to enforce all provisions of this Act as described
4 in subsection (c).

5 (c) CIVIL PENALTIES.—In addition to any other
6 sanctions or remedies that may be available under any
7 provision of Federal law, in the case of a regulated entity
8 or service provider that violates this section, subpart D
9 of part 160 of title 45, Code of Federal Regulations (or
10 any successor regulations), shall apply to the regulated en-
11 tity or service provider with respect to such violation of
12 this section in the same manner that such subpart applies
13 to a person with respect to a violation of part 160 of title
14 45, Code of Federal Regulations (or any successor regula-
15 tions).

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

24 (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-

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

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

6 (a) TIME AND MANNER OF ACCESS.—In applying
 7 section 13405(e) of the Health Information Technology
 8 for Economic and Clinical Health Act (42 U.S.C.
 9 17935(e)) or section 164.524(c)(3)(ii) of title 45, Code of
 10 Federal Regulations (or any successor regulations), in the
 11 case that an individual requests that a covered entity or
 12 any business associate of a covered entity transmit,
 13 produce, or provide access to a copy of the individual's
 14 protected health information to a person, including an en-
 15 tity, designated by the individual, and except where per-
 16 mitted without authorization under section 164.506(c) of
 17 title 45, Code of Federal Regulations (or any successor
 18 regulations)—

19 (1) the individual's request shall meet all re-
 20 quirements of a valid authorization under section
 21 164.508(b) of title 45, Code of Federal Regulations
 22 (or any successor regulations); and

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

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

3 (A) paying fees, in accordance with appli-
 4 cable State law and consistent with subsection
 5 (b), in advance of such transmittal, production,
 6 or access; and

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

12 (b) FEES.—

13 (1) IN GENERAL.—In applying section
 14 13405(e)(3) of the Health Information Technology
 15 for Economic and Clinical Health Act (42 U.S.C.
 16 17935(e)(3)) or section 164.524(c)(4) of title 45,
 17 Code of Federal Regulations (or any successor regu-
 18 lations), each such section shall apply only—

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

22 (i) the individual, or the individual's
 23 personal representative for health care pur-
 24 poses as described in section 164.502(g) of

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

3 (ii) subject to paragraph (2) and sec-
4 tion 164.510(b) of title 45, Code of Fed-
5 eral Regulations (or any successor regula-
6 tion), any other person identified in, and
7 subject to the limitations of, such section;
8 or

9 (iii) the individual's health care pro-
10 vider or the business associates of such
11 provider; and

12 (B) as directed by the individual, to the
13 electronic transmittal of the individual's elec-
14 tronic health record to the patient portal or mo-
15 bile medical application used and maintained by
16 the individual's health care provider or for the
17 health care provider by its business associate.

18 (2) ADDITIONAL LIMITATIONS.—In the case of
19 the provision of access to, or the production, copy-
20 ing, or transmittal of, protected health information
21 under paragraph (1)(A) directly to a person de-
22 scribed in clause (ii) of such paragraph, such pro-
23 tected health information shall, in accordance with
24 section 164.510(b) of title 45, Code of Federal Reg-

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

3 (A) directly relevant to the person’s in-
4 volvement with the care of the individual or
5 with the payment relevant to the care of the in-
6 dividual; or

7 (B) needed for notification purposes de-
8 scribed in such section.

9 (c) DEFINITIONS.—In this section, the terms “busi-
10 ness associate”, “covered entity”, “health care provider”,
11 “individual”, “person”, and “protected health informa-
12 tion” have the meanings given such terms in section
13 160.103 of title 45, Code of Federal Regulations (or any
14 successor regulations).

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

19 **SEC. 4. CONFIDENTIALITY OF RECORDS.**

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

22 (1) in subsection (a), by striking “subsection
23 (b)” and inserting “the HIPAA regulations”;

24 (2) in subsection (b)—

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

5 (B) by striking “(b) PERMITTED DISCLO-
 6 SURE” and all that follows through “(2) METH-
 7 OD FOR DISCLOSURE—Whether” and inserting
 8 the following:

9 “(b) PERMITTED DISCLOSURE.—Whether”;

10 (3) in subsection (c), in the matter preceding
 11 paragraph (1), by striking “subsection (b)(2)(C)”
 12 and inserting “subsection (b)(3)”; and

13 (4) in subsection (g), by striking “subsection
 14 (b)(2)(C)” and inserting “subsection (b)(3)”.

15 **SEC. 5. NAS STUDY ON COMPENSATION TO PATIENTS FOR**
 16 **SHARING IDENTIFIABLE DATA FOR RE-**
 17 **SEARCH PURPOSES.**

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

1 (b) INCLUSIONS.—The study conducted pursuant to
2 the contract under subsection (a) shall include an exam-
3 ination of—

4 (1) the risks to patient privacy posed by the in-
5 tegration of identifiable, de-identified, and aggre-
6 gated health information into datasets used for re-
7 search;

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

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

13 (4) ethical considerations for compensating pa-
14 tients for use of their identifiable and de-identified
15 health data;

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

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

21 **SEC. 6. PATIENT NOTIFICATION REQUIREMENTS UNDER**
22 **THE HIPAA PRIVACY REGULATIONS.**

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

1 the patient right of access under section 164.524 of title
2 45, Code of Federal Regulations (or any successor regula-
3 tions) shall—

4 (1) provide a written plain language notification
5 to such individual prior to accessing such informa-
6 tion—

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

10 (B) that includes an explanation of how
11 and to which entities such protected health in-
12 formation may be redisclosed; and

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

16 (b) PATIENT NOTIFICATION REGARDING WELLNESS
17 DATA.—

18 (1) IN GENERAL.—Any regulated entity or serv-
19 ice provider who offers digital technology that gen-
20 erates wellness data about individuals shall, with re-
21 spect to each individual who uses such technology—

22 (A) provide a written plain language notifi-
23 cation to the individual in advance of initiating
24 the generation of such data that such data will

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

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

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

10 (c) DEFINITIONS.—In this section—

11 (1) the terms “business associate”, “covered en-
12 tity”, and “protected health information” have the
13 meanings given such terms in section 160.103 of
14 title 45, Code of Federal Regulations (or any suc-
15 cessor regulations);

16 (2) the term “HIPAA privacy regulation” has
17 the meaning given such term in section 1180(b)(3)
18 of the Social Security Act (42 U.S.C. 1320d-
19 9(b)(3)); and

20 (3) the terms “regulated entity” and “service
21 provider” have the meanings given such terms in
22 section 2.

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

1 **SEC. 7. MINIMUM NECESSARY GUIDANCE.**

2 Not later than 1 year after the date of enactment
3 of this Act, the Secretary of Health and Human Services
4 shall publish guidance on the application of the minimum
5 necessary standard to data used for artificial intelligence
6 and other machine learning applications and relevant re-
7 quirements, including health data interoperability require-
8 ments under section 3001(c)(9) of the Public Health Serv-
9 ice Act (42 U.S.C. 300jj–11(c)(9)) and the use of limited
10 data sets pursuant to section 13405(b) of the HITECH
11 Act (42 U.S.C. 17935(b)).

12 **SEC. 8. DE-IDENTIFIED INFORMATION.**

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

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

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

1 164.514(b) of title 45, Code of Federal Regulations
2 (or any successor regulations);

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

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

15 (c) DEFINITIONS.—In this section—

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

18 (2) the terms “business associate”, “covered en-
19 tity”, and “individually identifiable health informa-
20 tion” have the meanings given such terms in section
21 160.103 of title 45, Code of Federal Regulations (or
22 any successor regulations); and

23 (3) the term “privacy enhancing technologies”
24 means any software or hardware solution, technical
25 process, or other technological means of mitigating

1 individuals' privacy risks arising from data proc-
2 essing by enhancing predictability, manageability,
3 disassociability, and confidentiality.

4 **SEC. 9. PREEMPTION.**

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

○