

STATE OF NEW YORK

1633--A

2025-2026 Regular Sessions

IN SENATE

January 13, 2025

Introduced by Sens. FERNANDEZ, CLEARE, COMRIE, FAHY, GOUNARDES, HARCHAM, JACKSON, KRUEGER, LIU, SALAZAR -- read twice and ordered printed, and when printed to be committed to the Committee on Health -- recommitted to the Committee on Health in accordance with Senate Rule 6, sec. 8 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the public health law, in relation to providing additional protections for sensitive health information and requiring all health information networks, electronic health records systems, and health care providers to provide patients with a right to restrict the disclosures of such patient's health information

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The public health law is amended by adding two new sections 25 and 26 to read as follows:

§ 25. Privacy of information disclosed through health information networks. 1. Definitions. For purposes of this section:

(a) "Business associate" shall have the same meaning as set forth in 45 CFR 160.103.

(b) "Codified sensitive information" means patient information that, by associated standard codes commonly used in the exchange of patient information including, but not limited to ICD-10 or SNOMED, can be identified as sensitive information in accordance with subdivision three of this section.

(c) "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity that delivered the health care and the patient who received the care, and such term shall not include any of the exceptions set forth in the definition of "disclosure to any other person" as defined in paragraph (e) of subdivision one of section eighteen of this chapter.

EXPLANATION--Matter in italics (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD04417-03-6

1 (d) "Electronic health records system" means any entity operating in
2 the state of New York that electronically stores or maintains patient
3 information, electronic health records, personal health records, health
4 care claims, or payment and other administrative data on behalf of a
5 health care provider, health care service plan, pharmaceutical company,
6 contractor, or employer.

7 (e) "Health care provider" shall have the same meaning as set forth in
8 paragraph (b) of subdivision one of section eighteen of this title and
9 for purposes of this section shall refer to health care providers that
10 are located in the state of New York and use a health information
11 network to receive, hold or exchange patient information on their
12 behalf.

13 (f) "Health information network" shall mean any entity, including a
14 health information technology developer of certified health information
15 technology, that receives, holds or exchanges patient information in
16 electronic form on behalf of a health care provider and makes such
17 information available to two or more individuals or entities that are
18 unaffiliated with the health care provider for purposes of treatment,
19 payment, or health care operations, as those terms are defined under
20 HIPAA, or a qualified health information network as established under
21 TEFCA, which exchanges patient information on behalf of a health care
22 provider located in the state of New York. An entity may qualify as a
23 "health information network" irrespective of whether such entity
24 receives funding from the department. The term "health information
25 network" shall not include:

26 (i) a health care provider;
27 (ii) an entity that makes patient information available solely:
28 (1) from one health care provider to a single health care provider as
29 part of a referral, prescription, or consultation;
30 (2) as necessary for the payment of a health care claim;
31 (3) among affiliates of a single health care provider;
32 (4) to individuals and entities under contract with the entity who
33 meet the definition of a "business associate" under HIPAA and who proc-
34 ess patient information only as directed by a health care provider and
35 do not disclose patient information; or

36 (5) as necessary to operate clinical data registries, provide organ
37 donation coordination services and other similar services as deemed
38 appropriate by the department in regulation;

39 (iii) a health insurer or a health maintenance organization, when
40 acting as a health insurer, to the extent it exchanges patient informa-
41 tion via HIPAA standard transactions; and

42 (iv) an entity that makes patient information available solely to and
43 between health information networks and has no ability to access, modi-
44 fy, or further disclose patient information, including, but not limited
45 to, the recognized coordinating entity under TEFCA.

46 (g) "HIPAA" means the Health Insurance Portability and Accountability
47 Act of 1996 and its implementing regulations at 45 C.F.R. Parts 160,
48 162, and 164.

49 (h) "Non-codified sensitive information" means patient information
50 that contains or reveals sensitive information, but that is not associ-
51 ated with standardized codes and shall include, but is not limited to
52 notes, visit summaries, laboratory results and images.

53 (i) "Patient information" shall have the same meaning as set forth in
54 paragraph (e) of subdivision one of section eighteen of this chapter.

55 (j) "Qualified person" shall have the same meaning as set forth in
56 paragraph (g) of subdivision one of section eighteen of this title.

(k) "Sensitive information" means patient information that contains or reveals reproductive health services as defined in paragraph (a) of subdivision one of section sixty-five hundred thirty-one-b of the education law, gender-affirming care as defined in paragraph (c) of subdivision one of section sixty-five hundred thirty-one-b of the education law, care protected under 42 CFR part 2, diagnosis and treatment for a sexually transmitted infection or HIV, mental health services, alcohol or substance use treatment, and any other health care services determined by the commissioner through regulations, in consultation with health care providers, patient advocates, health information networks and other relevant stakeholders.

(l) "TEFCA" means the Trusted Exchange Framework and Common Agreement authorized by the 21st Century Cures Act.

2. Patient right to restrict disclosures by health information networks. Within one hundred eighty days from the effective date of this section, the department shall establish rules and regulations requiring any health information network to:

(a) provide qualified persons with the means of requesting, without undue effort, restrictions on disclosures of patient information from all health information networks;

(b) subject to any regulatory exceptions established by the department, abide by the terms of a qualified person's requested restriction made under paragraph (a) of this subdivision; and

(c) subject to any regulatory exceptions established by the department, provide or cause to be provided to qualified persons, upon request, a report or notifications detailing disclosures of the applicable patient's patient information by or through all health information networks.

3. Additional protections for codified sensitive information by health information networks. (a) Within one hundred eighty days from the effective date of this section, the department shall establish rules and regulations, consistent with state and federal law and regulations, including but not limited to article thirty-three of the mental hygiene law and section twenty-seven hundred eighty-two of this chapter, requiring any health information network to:

(i) develop the capacity to limit the disclosure of codified sensitive information while allowing for the disclosure of a patient's other health information;

(ii) when directed by a qualified person, limit user access privileges to codified sensitive information to only those HIPAA covered entities whom the qualified person has specifically authorized to access the codified sensitive information;

(iii) provide the ability to automatically disable access to codified sensitive information by an individual or entity located outside the state of New York as directed by a qualified person; and

(iv) unless otherwise ordered by a court of competent jurisdiction, notify the qualified person and the provider who rendered the health care documented in the codified sensitive information at least thirty days prior to complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons for codified sensitive information.

(b) Such rules and regulations shall also:

(i) establish a list of procedure codes, diagnosis codes, medication codes, and other appropriate codes that constitute codified sensitive information;

(ii) set forth exceptions to the requirement to block the disclosure of codified sensitive information as required by paragraph (a) of this

subdivision, including for disclosures to individuals and entities under contract with a health information network who meet the definition of a "business associate" under HIPAA and who do not re-disclose such patient information; and

(iii) establish guidelines for the authorization necessary to limit disclosure of codified sensitive information pursuant to subparagraphs (ii) and (iii) of paragraph (a) of this subdivision.

4. Additional protections for sensitive information by electronic health records systems. (a) Within one hundred eighty days of the effective date of this section, the department shall establish rules and regulations, consistent with state and federal law and regulations, including but not limited to article thirty-three of the mental hygiene law and section twenty-seven hundred eighty-two of this chapter, requiring any electronic health records system to:

(i) develop the capacity to provide qualified persons with the means of requesting, without undue effort, restrictions on disclosures of patient information;

(ii) develop the capacity to limit the disclosure of codified sensitive information while allowing for the disclosure of a patient's other health information;

(iii) when directed by a qualified person, limit user access privileges to codified sensitive information to only those HIPAA covered entities whom the qualified person has specifically authorized to access the sensitive information;

(iv) provide the ability to automatically disable access to codified sensitive information by an individual or entity located outside the state of New York as directed by a qualified person; and

(v) unless otherwise ordered by a court of competent jurisdiction, notify the qualified person and the provider who rendered the health care documented in the codified sensitive information at least thirty days prior to complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons for codified sensitive information.

(b) Within one year of the effective date of this section, the department shall establish rules and regulations, consistent with state and federal law and regulations, including but not limited to article thirty-three of the mental hygiene law and section twenty-seven hundred eighty-two of this chapter, requiring any electronic health records system to:

(i) develop the capacity to limit the disclosure of non-codified sensitive information while allowing for the disclosure of a patient's other health information;

(ii) when directed by a qualified person, limit user access privileges to non-codified sensitive information to only those HIPAA covered entities whom the qualified person has specifically authorized to access the non-codified sensitive information;

(iii) provide the ability to automatically disable access to non-codified sensitive information by an individual or entity located outside the state of New York as directed by a qualified person; and

(iv) unless otherwise ordered by a court of competent jurisdiction, notify the qualified person and the provider who rendered the health care documented in the non-codified sensitive information at least thirty days prior to complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons for non-codified sensitive information.

(c) The rules and regulations required by paragraphs (a) and (b) of this subdivision shall also:

1 (i) set forth exceptions to the requirement to block the disclosure of
2 codified and non-codified sensitive information as required by para-
3 graphs (a) and (b) of this subdivision, including for disclosures to
4 individuals and entities under contract with a health information
5 network who meet the definition of a "business associate" under HIPAA
6 and who do not re-disclose such patient information; and

7 (ii) establish guidelines for the authorization necessary to limit
8 disclosure of codified and non-codified sensitive information pursuant
9 to subparagraphs (iii) and (iv) of paragraph (a) and subparagraphs (ii)
10 and (iii) of paragraph (b) of this section.

11 5. Authorization. Notwithstanding section eighteen of this title and
12 subdivision twenty-three of section sixty-five hundred thirty of the
13 education law, a health information network that abides by a qualified
14 person's request to limit disclosure of sensitive information shall not
15 be otherwise required to obtain authorization for the disclosure of
16 patient information, unless authorization is required in accordance with
17 subdivisions three or four of this section, article twenty-seven-F of
18 this chapter, the provisions of section seventeen of this title related
19 to prohibiting the release to an infant patient's parent or guardian of
20 information related to the treatment of such infant patient for venereal
21 disease or the performance of an abortion operation upon such infant
22 patient, section 33.13 of the mental hygiene law, section seventy-nine-1
23 of the civil rights law, section three hundred ninety-four-e of the
24 general business law, 42 CFR part 2, HIPAA, or other relevant federal,
25 state, or local laws.

26 § 26. Privacy of patient information held by health care providers.

27 1. Definitions. For purposes of this section:

28 (a) "Disclosure" means the release, transfer, provision of access to,
29 or divulging in any manner of information outside the entity that deliv-
30 ered the health care and the patient who received the care, and such
31 term shall not include any of the exceptions set forth in the definition
32 of "disclosure to any other person" as defined in paragraph (e) of
33 subdivision one of section eighteen of this chapter.

34 (b) "Health care provider" shall have the same meaning as set forth in
35 paragraph (b) of subdivision one of section eighteen of this chapter.

36 (c) "HIPAA" shall have the same meaning as set forth in paragraph (g)
37 of subdivision one of section twenty-five of this title.

38 (d) "Patient information" shall have the same meaning as set forth in
39 paragraph (e) of subdivision one of section eighteen of this title.

40 (e) "Qualified person" shall have the same meaning as set forth in
41 paragraph (g) of subdivision one of section eighteen of this title.

42 (f) "Sensitive information" shall have the same meaning as set forth
43 in paragraph (k) of subdivision one of section twenty-five of this
44 title.

45 2. Patient right to restrict disclosures by health care providers.

46 (a) Within one hundred eighty days from the effective date of this
47 subdivision, the department shall establish rules and regulations that
48 require health care providers to take reasonable steps to:

49 (i) provide qualified persons with the means of requesting
50 restrictions on disclosures of patient information consistent with the
51 obligations imposed by section twenty-five of this title;

52 (ii) notify qualified persons of their right to restrict the disclo-
53 sure of patient information consistent with the capabilities developed
54 by the electronic health records system utilized by the health care
55 provider;

1 (iii) subject to any regulatory exceptions established by the depart-
2 ment, abide by the terms of a qualified person's requested restriction;
3 and

4 (iv) unless otherwise ordered by a court of competent jurisdiction,
5 notify the qualified person at least thirty days prior to complying with
6 a civil, criminal, or regulatory inquiry, investigation, subpoena, or
7 summons for sensitive information.

8 (b) Nothing in paragraph (a) of this subdivision shall create an
9 affirmative obligation on a health care provider to review non-codified
10 data created prior to the effective date of any rules and regulations
11 promulgated pursuant to this section.

12 (c) The department's rules and regulations shall set forth exceptions
13 to a qualified person's right to restrict disclosures and shall include,
14 at a minimum, exceptions for:

15 (i) disclosures to public health authorities located in the state of
16 New York in accordance with New York law;

17 (ii) disclosures necessary to facilitate payment of a health care
18 claim;

19 (iii) disclosures necessary to ensure that a provider is in compliance
20 with applicable quality of care, licensure or accreditation standards;
21 and

22 (iv) disclosures strictly necessary to fill a prescription or provide
23 a service.

24 (d) The department shall establish phase-in periods for health care
25 providers to implement the requirements of this subdivision, taking into
26 account the technical feasibility of implementing restrictions among
27 various sectors, including (i) small health care providers; and (ii)
28 health care providers in sectors that do not typically utilize certified
29 health information technology, as well as the time it takes for the
30 health information systems or electronic health record systems to devel-
31 op and implement the capacity to segment health records.

32 (e) The department shall provide guidance to health care providers,
33 including model notices health care providers may use to notify quali-
34 fied persons to permit them to exercise their rights under this subdivi-
35 sion. Such guidance shall recommend more prominent notices and means
36 for a qualified person to exercise their rights in health care settings
37 where sensitive information is frequently generated as part of patients'
38 health care records.

39 3. Authorization for a health care provider's disclosure of patient
40 information. Notwithstanding section eighteen of this title and subdivi-
41 sion twenty-three of section sixty-five hundred thirty of the education
42 law, if a health care provider has provided actual notice to a qualified
43 person of such person's right to restrict disclosures of patient infor-
44 mation in accordance with the requirements of subdivision two of this
45 section and abides by a qualified person's request to restrict disclo-
46 tures, no authorization shall be required for such health care provider
47 to disclose a patient's other patient information unless authorization
48 is required by this section or section twenty-five of this title, arti-
49 cle twenty-seven-F of this chapter, the provisions of section seventeen
50 of this title relating to prohibiting the release to an infant patient's
51 parent or guardian of information related to the treatment of such
52 infant patient for venereal disease or the performance of an abortion
53 operation upon such infant patient, section 33.13 of the mental hygiene
54 law, section seventy-nine-1 of the civil rights law, section three
55 hundred ninety-four-e of the general business law, 42 CFR part 2, HIPAA,
56 or other relevant federal, state, or local laws.

1 4. Authorization for a health care provider's request for patient
2 information. Notwithstanding section eighteen of this title and subdivi-
3 sion twenty-three of section sixty-five hundred thirty of the education
4 law, if a health care provider provides actual notice to qualified
5 persons that it makes routine requests for patient information from
6 other individuals or entities, no authorization shall be required to
7 make a request for patient information unless authorization is required
8 by this section or section twenty-five of this title, article
9 twenty-seven-F of this chapter, the provisions of section seventeen of
10 this title relating to prohibiting the release to an infant patient's
11 parent or guardian of information related to the treatment of such
12 infant patient for venereal disease or the performance of an abortion
13 operation upon such infant patient, section 33.13 of the mental hygiene
14 law, section seventy-nine-1 of the civil rights law, section three
15 hundred ninety-four-e of the general business law, 42 CFR part 2, HIPAA,
16 or other relevant federal, state, or local laws.

17 5. Disclosure of de-identified patient information. Nothing in this
18 section shall prohibit a health care provider's disclosure of de-identi-
19 fied patient information for the purposes of quality assurance or
20 improvement activities, clinical trials or research. For purposes of
21 this section, "de-identified" means that the information cannot identify
22 or be made to identify or be associated with a particular individual,
23 directly or indirectly and is subject to technical safeguards and poli-
24 cies and procedures that prevent re-identification, whether inten-
25 tionally or unintentionally, of any individual.

26 § 2. Nothing set forth in this act shall be construed as creating,
27 establishing, or authorizing a new private cause of action by an
28 aggrieved person against a health information network, electronic health
29 records system, or health care provider who has violated, or is alleged
30 to have violated, any provision of this act.

31 § 3. Severability. If any provision of this act, or any application of
32 any provision of this act, is held to be invalid, or ruled to violate or
33 be inconsistent with any applicable federal law or regulation, that
34 shall not affect the validity or effectiveness of any other provision of
35 this act, or of any other application of any provision of this act. It
36 is hereby declared to be the intent of the legislature that this act
37 would have been enacted even if such invalid provisions had not been
38 included herein.

39 § 4. This act shall take effect immediately.