

STATE OF NEW YORK

1633

2025-2026 Regular Sessions

IN SENATE

January 13, 2025

Introduced by Sen. FERNANDEZ -- read twice and ordered printed, and when printed to be committed to the Committee on Health

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 record 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:

1 Section 1. The public health law is amended by adding two new sections
2 25 and 26 to read as follows:

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

5 (a) "Business associate" shall have the same meaning as set forth in
6 45 CFR 160.103.

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

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

18 (d) "Electronic health records system" means any entity operating in
19 the state of New York that electronically stores or maintains patient
20 information, electronic health records, personal health records, health
21 care claims, or payment and other administrative data on behalf of a

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

LBD04417-02-5

1 health care provider, health care service plan, pharmaceutical company,
2 contractor, or employer.

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

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

22 (i) a health care provider;

23 (ii) an entity that makes patient information available solely:

24 (1) from one health care provider to a single health care provider as
25 part of a referral, prescription, or consultation;

26 (2) as necessary for the payment of a health care claim;

27 (3) among affiliates of a single health care provider;

28 (4) to individuals and entities under contract with the entity who
29 meet the definition of a "business associate" under HIPAA and who proc-
30 ess patient information only as directed by a health care provider and
31 do not disclose patient information; or

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

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

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

42 (g) "HIPAA" means the Health Insurance Portability and Accountability
43 Act of 1996 and its implementing regulations at 45 C.F.R. Parts 160,
44 162, and 164.

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

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

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

53 (k) "Sensitive information" means patient information that contains or
54 reveals reproductive health services as defined in paragraph (a) of
55 subdivision one of section sixty-five hundred thirty-one-b of the educa-
56 tion law, gender-affirming care as defined in paragraph (c) of subdivi-

sion 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.

(1) "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:

(i) set forth exceptions to the requirement to block the disclosure of codified and non-codified sensitive information as required by paragraphs (a) and (b) of this subdivision, including for disclosures to individuals and entities under contract with a health information

1 network who meet the definition of a "business associate" under HIPAA
2 and who do not re-disclose such patient information; and

3 (ii) establish guidelines for the authorization necessary to limit
4 disclosure of codified and non-codified sensitive information pursuant
5 to subparagraphs (iii) and (iv) of paragraph (a) and subparagraphs (ii)
6 and (iii) of paragraph (b) of this section.

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

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

23 1. Definitions. For purposes of this section:

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

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

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

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

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

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

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

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

45 (i) provide qualified persons with the means of requesting
46 restrictions on disclosures of patient information consistent with the
47 obligations imposed by section twenty-five of this article;

48 (ii) notify qualified persons of their right to restrict the disclo-
49 sure of patient information;

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

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

1 (b) The department's rules and regulations shall set forth exceptions
2 to a qualified person's right to restrict disclosures and shall include,
3 at a minimum, exceptions for:

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

6 (ii) disclosures necessary to facilitate payment of a health care
7 claim;

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

11 (iv) disclosures strictly necessary to fill a prescription or provide
12 a service.

13 (c) The department shall establish phase-in periods for health care
14 providers to implement the requirements of this subdivision, taking into
15 account the technical feasibility of implementing restrictions among
16 various sectors, including (i) small health care providers; and (ii)
17 health care providers in sectors that do not typically utilize certified
18 health information technology, as well as the time it takes for the
19 health information systems or electronic health record systems to devel-
20 op and implement the capacity to segment health records.

21 (d) The department shall provide guidance to health care providers,
22 including model notices health care providers may use to notify quali-
23 fied persons to permit them to exercise their rights under this subdivi-
24 sion. Such guidance shall recommend more prominent notices and means
25 for a qualified person to exercise their rights in health care settings
26 where sensitive information is frequently generated as part of patients'
27 health care records.

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

46 4. Authorization for a health care provider's request for patient
47 information. Notwithstanding section eighteen of this title and subdivi-
48 sion twenty-three of section sixty-five hundred thirty of the education
49 law, if a health care provider provides actual notice to qualified
50 persons that it makes routine requests for patient information from
51 other individuals or entities, no authorization shall be required to
52 make a request for patient information unless authorization is required
53 by this section or section twenty-five of this title, article
54 twenty-seven-F of this chapter, the provisions of section seventeen of
55 this title relating to prohibiting the release to an infant patient's
56 parent or guardian of information related to the treatment of such

1 infant patient for venereal disease or the performance of an abortion
2 operation upon such infant patient, section 33.13 of the mental hygiene
3 law, section seventy-nine-1 of the civil rights law, section three
4 hundred ninety-four-e of the general business law, 42 CFR part 2, HIPAA,
5 or other relevant federal, state, or local laws.

6 5. Disclosure of de-identified patient information. Nothing in this
7 section shall prohibit a health care provider's disclosure of de-identi-
8 fied patient information for the purposes of quality assurance or
9 improvement activities, clinical trials or research. For purposes of
10 this section, "de-identified" means that the information cannot identify
11 or be made to identify or be associated with a particular individual,
12 directly or indirectly and is subject to technical safeguards and poli-
13 cies and procedures that prevent re-identification, whether inten-
14 tionally or unintentionally, of any individual.

15 § 2. Severability. If any provision of this act, or any application of
16 any provision of this act, is held to be invalid, or ruled to violate or
17 be inconsistent with any applicable federal law or regulation, that
18 shall not affect the validity or effectiveness of any other provision of
19 this act, or of any other application of any provision of this act. It
20 is hereby declared to be the intent of the legislature that this act
21 would have been enacted even if such invalid provisions had not been
22 included herein.

23 § 3. This act shall take effect immediately.