

STATE OF NEW YORK

1633--B

Cal. No. 140

2025-2026 Regular Sessions

IN SENATE

January 13, 2025

Introduced by Sens. FERNANDEZ, CLEARE, COMRIE, FAHY, GONZALEZ, GOUNARDES, HARCKHAM, 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 -- recommitted to the Committee on Rules in accordance with Senate Rule 6, sec. 8 -- reported favorably from said committee, ordered to a third reading, passed by Senate and delivered to the Assembly, recalled, vote reconsidered, restored to third reading, amended and ordered reprinted, retaining its place in the order of third reading

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:

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-

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

LBD04417-08-6

1 ered the health care and the patient who received the care, and such
2 term shall not include any of the exceptions set forth in the definition
3 of "disclosure to any other person" as defined in paragraph (e) of
4 subdivision one of section eighteen of this chapter.

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

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

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

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

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

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

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

50 (g) "HIPAA" means the Health Insurance Portability and Accountability
51 Act of 1996 and its implementing regulations at 45 C.F.R. Parts 160,
52 162, and 164.

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

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

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

5 (k) "Sensitive information" means patient information that contains or
6 reveals reproductive health services as defined in paragraph (a) of
7 subdivision one of section sixty-five hundred thirty-one-b of the educa-
8 tion law, gender-affirming care as defined in paragraph (c) of subdivi-
9 sion one of section sixty-five hundred thirty-one-b of the education
10 law, care protected under 42 CFR part 2, diagnosis and treatment for a
11 sexually transmitted infection or HIV, mental health services, alcohol
12 or substance use treatment, and any other health care services deter-
13 mined by the commissioner through regulations, in consultation with
14 health care providers, patient advocates, health information networks
15 and other relevant stakeholders.

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

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

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

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

28 (c) subject to any regulatory exceptions established by the depart-
29 ment, provide or cause to be provided to qualified persons, upon
30 request, a report or notifications detailing disclosures of the applica-
31 ble patient's patient information by or through all health information
32 networks.

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

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

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

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

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

55 (b) Such rules and regulations shall also:

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

4 (ii) set forth exceptions to the requirement to block the disclosure
5 of codified sensitive information as required by paragraph (a) of this
6 subdivision, including for disclosures to individuals and entities under
7 contract with a health information network who meet the definition of a
8 "business associate" under HIPAA and who do not re-disclose such patient
9 information;

10 (iii) set forth standards for which sensitive health information that
11 has been restricted pursuant to paragraph (a) of this subdivision can be
12 made available to a treating health care provider to the extent strictly
13 necessary to treat a patient who is experiencing a bona fide medical
14 emergency when the patient or other qualified person is unable to
15 consent to disclosure as a result of such bona fide medical emergency or
16 when the patient is unable to consent and obtaining consent from another
17 qualified person would cause a delay in treatment that would result,
18 within reasonable medical probability, in serious jeopardy to the
19 patient's health or life; provided that any sensitive information made
20 available pursuant to this subparagraph shall not be integrated into the
21 patient's other health care information and shall revert to the quali-
22 fied person's direction under paragraph (a) of this subdivision when the
23 bona fide medical emergency abates or when the patient regains deci-
24 sional capacity or another qualified person is available to consent for
25 them; provided, further that the treating health care provider may
26 include sensitive information that is relevant to the patient's current
27 diagnosis and treatment in their own entry into the patient's electronic
28 health record; and provided, further that health information networks
29 shall maintain, and proactively share with the patient, the name of the
30 treating health care provider who accessed the sensitive health informa-
31 tion, the health care facility they are affiliated with, the date and
32 time of the access, and the nature of the bona fide medical emergency;
33 and

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

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

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

47 (ii) develop the capacity to limit the disclosure of codified sensi-
48 tive information while allowing for the disclosure of a patient's other
49 health information;

50 (iii) when directed by a qualified person, limit user access privi-
51 leges to codified sensitive information to only those HIPAA covered
52 entities whom the qualified person has specifically authorized to access
53 the sensitive information;

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

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

6 (b) Within one year of the effective date of this section, the depart-
7 ment shall establish rules and regulations, consistent with state and
8 federal law and regulations, including but not limited to article thir-
9 ty-three of the mental hygiene law and section twenty-seven hundred
10 eighty-two of this chapter, requiring any electronic health records
11 system to:

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

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

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

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

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

30 (i) set forth standards for which sensitive health information that
31 has been restricted pursuant to paragraph (a) of this subdivision can be
32 made available to a treating health care provider to the extent strictly
33 necessary to treat a patient who is experiencing a bona fide medical
34 emergency when the patient or other qualified person is unable to
35 consent to disclosure as a result of such bona fide medical emergency or
36 when the patient is unable to consent and obtaining consent from another
37 qualified person would cause a delay in treatment that would result,
38 within reasonable medical probability, in serious jeopardy to the
39 patient's health or life; provided that any sensitive information made
40 available pursuant to this subparagraph shall not be integrated into the
41 patient's other health care information and shall revert to the quali-
42 fied person's direction under paragraph (a) of this subdivision when the
43 bona fide medical emergency abates or when the patient regains deci-
44 sional capacity or another qualified person is available to consent for
45 them; provided, further that the treating health care provider may
46 include sensitive information that is relevant to the patient's current
47 diagnosis and treatment in their own entry into the patient's electronic
48 health record; and provided, further that health information networks
49 shall maintain, and proactively share with the patient, the name of the
50 treating health care provider who accessed the sensitive health informa-
51 tion, the health care facility they are affiliated with, the date and
52 time of the access, and the nature of the bona fide medical emergency;

53 (ii) set forth exceptions to the requirement to block the disclosure
54 of codified and non-codified sensitive information as required by para-
55 graphs (a) and (b) of this subdivision, including for disclosures to
56 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 (iii) 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 (iii) and (iv) of paragraph (b) of this subdivision.

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 title.

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 title.

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 title;

48 (ii) notify qualified persons of their right to restrict the disclo-
49 sure of patient information consistent with the capabilities developed
50 by the electronic health records system utilized by the health care
51 provider;

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

54 (iv) unless otherwise ordered by a court of competent jurisdiction,
55 notify the qualified person at least thirty days prior to complying with

1 a civil, criminal, or regulatory inquiry, investigation, subpoena, or
2 summons for sensitive information; and

3 (v) immediately following any access to sensitive health information
4 pursuant to subparagraph (iii) of paragraph (b) of subdivision three of
5 section twenty-five of this title or subparagraph (i) of paragraph (c)
6 of subdivision four of section twenty-five of this title, document, in
7 writing, and proactively share with the patient, the name of the treat-
8 ing health care provider who accessed the sensitive health information,
9 the health care facility they are affiliated with, the date and time of
10 the access, and the nature of the bona fide medical emergency.

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

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

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

20 (ii) disclosures necessary to facilitate payment of a health care
21 claim;

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

25 (iv) disclosures strictly necessary to fill a prescription or provide
26 a service.

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

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

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

1 law, section seventy-nine-1 of the civil rights law, section three
2 hundred ninety-four-e of the general business law, 42 CFR part 2, HIPAA,
3 or other relevant federal, state, or local laws.

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

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

29 6. Penalties. A health care provider shall not be subject to any
30 penalties based solely on a health information network's failure to
31 comply with section twenty-five of this title.

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

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

45 § 4. This act shall take effect immediately.