STATE OF NEW YORK

2613--A

2025-2026 Regular Sessions

IN ASSEMBLY

January 21, 2025

Introduced by M. of A. LUNSFORD, TAPIA, LEVENBERG, GALLAGHER, LASHER, R. CARROLL, SIMON, GLICK, SIMONE, STECK, KASSAY, TORRES, GONZALEZ-ROJAS, BURROUGHS, ROSENTHAL, HEVESI, LAVINE, REYES, McDONALD, SEAWRIGHT, BRONSON, KELLES, LEE, SHIMSKY, GRIFFIN -- read once and referred to the Committee on Health -- recommitted to the Committee on Health in accordance with Assembly Rule 3, sec. 2 -- 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

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

LBD04417-07-6

of "disclosure to any other person" as defined in paragraph (e) of subdivision one of section eighteen of this chapter.

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

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

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

(i) a health care provider;

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

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

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

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

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

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

(iii) a health insurer or a health maintenance organization, when acting as a health insurer, to the extent it exchanges patient information via HIPAA standard transactions; and

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

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

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

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

(j) "Qualified person" shall have the same meaning as set forth in 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;

(iii) set forth standards for which sensitive health information that has been restricted pursuant to paragraph (a) of this subdivision can be made available to a treating health care provider to the extent strictly necessary to treat a patient who is experiencing a bona fide medical emergency when the patient or other qualified person is unable to consent to disclosure as a result of such bona fide medical emergency or when the patient is unable to consent and obtaining consent from another qualified person would cause a delay in treatment that would result, within reasonable medical probability, in serious jeopardy to the patient's health or life; provided that any sensitive information made available pursuant to this subparagraph shall not be integrated into the patient's other health care information and shall revert to the qualified person's direction under paragraph (a) of this subdivision when the bona fide medical emergency abates or when the patient regains decisional capacity or another qualified person is available to consent for them; provided, further that the treating health care provider may include sensitive information that is relevant to the patient's current diagnosis and treatment in their own entry into the patient's electronic health record; and provided, further that health information networks shall maintain, and proactively share with the patient, the name of the treating health care provider who accessed the sensitive health information, the health care facility they are affiliated with, the date and time of the access, and the nature of the bona fide medical emergency; and

(iv) 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 standards for which sensitive health information that has been restricted pursuant to paragraph (a) of this subdivision can be made available to a treating health care provider to the extent strictly necessary to treat a patient who is experiencing a bona fide medical emergency when the patient or other qualified person is unable to consent to disclosure as a result of such bona fide medical emergency or when the patient is unable to consent and obtaining consent from another qualified person would cause a delay in treatment that would result, within reasonable medical probability, in serious jeopardy to the patient's health or life; provided that any sensitive information made available pursuant to this subparagraph shall not be integrated into the patient's other health care information and shall revert to the qualified person's direction under paragraph (a) of this subdivision when the bona fide medical emergency abates or when the patient regains decisional capacity or another qualified person is available to consent for them; provided, further that the treating health care provider may include sensitive information that is relevant to the patient's current diagnosis and treatment in their own entry into the patient's electronic health record; and provided, further that health information networks shall maintain, and proactively share with the patient, the name of the treating health care provider who accessed the sensitive health information, the health care facility they are affiliated with, the date and time of the access, and the nature of the bona fide medical emergency;

(ii) 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 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 and non-codified sensitive information pursuant to subparagraphs (iii) and (iv) of paragraph (a) and subparagraphs (ii), (iii) and (iv) of paragraph (b) of this subdivision.

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

§ 26. Privacy of patient information held by health care providers. 1. Definitions. For purposes of this section:

(a) "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 title.

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

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

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

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

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

2. Patient right to restrict disclosures by health care providers. (a) Within one hundred eighty days from the effective date of this subdivision, the department shall establish rules and regulations that require health care providers to take reasonable steps to:

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

(ii) notify qualified persons of their right to restrict the disclosure of patient information consistent with the capabilities developed by the electronic health records system utilized by the health care provider;

(iii) subject to any regulatory exceptions established by the department, abide by the terms of a qualified person's requested restriction;

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

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

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

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

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

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

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

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

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

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

3. Authorization for a health care provider's disclosure of patient information. Notwithstanding section eighteen of this title and subdivision twenty-three of section sixty-five hundred thirty of the education law, if a health care provider has provided actual notice to a qualified person of such person's right to restrict disclosures of patient information in accordance with the requirements of subdivision two of this section and abides by a qualified person's request to restrict disclosures, no authorization shall be required for such health care provider to disclose a patient's other patient information unless authorization is required by this section or section twenty-five of this title, article twenty-seven-F of this chapter, the provisions of section seventeen of this title relating to prohibiting the release to an infant patient's parent or guardian of information related to the treatment of such infant patient for venereal disease or the performance of an abortion operation upon such infant patient, section 33.13 of the mental hygiene law, section seventy-nine-l of the civil rights law, section three

hundred ninety-four-e of the general business law, 42 CFR part 2, HIPAA, or other relevant federal, state, or local laws.

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

5. Disclosure of de-identified patient information. Nothing in this section shall prohibit a health care provider's disclosure of de-identified patient information for the purposes of quality assurance or improvement activities, clinical trials or research. For purposes of this section, "de-identified" means that the information cannot identify or be made to identify or be associated with a particular individual, directly or indirectly and is subject to technical safeguards and policies and procedures that prevent re-identification, whether intentionally or unintentionally, of any individual.

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

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

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

§ 4. This act shall take effect immediately.