STATE OF NEW YORK

4983--B

2023-2024 Regular Sessions

IN ASSEMBLY

February 27, 2023

Introduced by M. of A. L. ROSENTHAL, CUNNINGHAM -- read once and referred to the Committee on Science and Technology -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- again reported from said committee with amendments, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law, in relation to providing for the protection of health information

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

Section 1. The general business law is amended by adding a new article 42 to read as follows:

§ 1100. Definitions. As used in this article, the following terms shall have the following meanings:

1. "Deidentified information" means information that cannot reasonably be used to infer information about, or otherwise be linked to a particular individual, household, or device, provided that the regulated entity or service provider that processes the information:

(a) Implements reasonable technical safeguards to ensure that the information cannot be associated with an individual, household, or device;

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

LBD01105-07-3

(b) Publicly commits to process the information only as deidentified information and not attempt to reidentify the information, except that the regulated entity or service provider may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this section; and

(c) Contractually obligates any recipient of the deidentified information to comply with all requirements of this section.

2. "Regulated health information" means any information that is reasonably linkable to an individual, or a device, and is collected or processed in connection with the physical or mental health of an individual. Location or payment information that relates to an individual's physical or mental health or any inference drawn or derived about an individual's physical or mental health that is reasonably linkable to an individual, or a device, shall be considered, without limitation, regulated health information. Regulated health information shall not include deidentified information.

3. "Process" or "processing" means an operation or set of operations performed on regulated health information, including but not limited to the collection, use, access, sharing, sale, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, disposal, licensing, destruction, deletion, modification, or deidentification of regulated health information.

4. "Regulated entity" means any entity that (a) controls the processing of regulated health information of an individual who is a New York resident, (b) controls the processing of regulated health information of an individual who is physically present in New York while that individual is in New York, or (c) is located in New York and controls the processing of regulated health information of an individual. A regulated entity may also be a service provider depending upon the context in which regulated health information is processed.

5. "Sell" means to share regulated health information for monetary or other valuable consideration. Selling does not include the sharing of regulated health information for monetary or other valuable consideration to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets.

6. "Service provider" means any person or entity that processes regulated health information on behalf of a regulated entity. A service provider may also be a regulated entity depending upon the context in which regulated health information is processed.

7. "Third party" means a person or entity other than the individual, regulated entity, or service provider involved in a transaction or occurrence that involves regulated health information. A third party may also be a regulated entity or service provider depending upon the context in which regulated health information is processed.

§ 1101. Requirements for communications to individuals. All notices, disclosures, forms, and other communications to individuals provided pursuant to this article shall comply with the following:

1. In general, all communications shall use plain, straightforward language, avoiding technical or legal jargon, and must be provided through an interface regularly used in conjunction with the regulated entity's product or service.

2. All communications shall be reasonably accessible to individuals with disabilities, including by:

(a) utilizing digital accessibility tools;

(b) for notices, complying with generally recognized industry standards, including, but not limited to, the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Web Consortium, incorporated herein by reference; and

(c) for other communications, providing information about how an individual with a disability may access the communication in an alternative format.

3. All communications shall be available in the languages in which the regulated entity provides information via its website and services. Any direct communication to an individual shall be provided in the language in which the individual ordinarily interacts with the regulated entity or its service provider.

4. A regulated entity shall make any notice for processing pursuant to a permissible purpose, pursuant to subparagraph (ii) of paragraph (b) of subdivision one of section eleven hundred two of this article, or form for processing pursuant to authorization, pursuant to subparagraph (i) of paragraph (b) of subdivision one of section eleven hundred two of this article, publicly available on its website. If an authorization form is customized for each individual, the regulated entity may instead publicly post a sample authorization form on its website.

§ 1102. Lawfulness of processing regulated health information. 1. In general, it shall be unlawful for a regulated entity to:

(a) sell an individual's regulated health information to a third party; or

(b) otherwise process an individual's regulated health information unless:

(i) The individual has provided valid authorization for such processing; or

(ii) Processing of an individual's regulated health information is strictly necessary for the purpose of:

(A) providing a product or service requested by such individual;

(B) conducting the regulated entity's internal business operations, which exclude any activities related to marketing, advertising, research and development, or providing products or services to third parties;

(C) protecting against malicious, fraudulent, or illegal activity;

(D) detecting, responding to, or preventing security incidents or threats;

(E) protecting the vital interests of an individual or the public interest in the area of public health;

(F) investigating, establishing, exercising, preparing for, or defending legal claims; or

(G) complying with the regulated entity's legal obligations.

2. A regulated entity that processes regulated health information pursuant to valid authorization as required by subparagraph (i) of paragraph (b) of subdivision one of this section shall comply with the following:

(a) A request for authorization to process an individual's regulated health information shall:

(i) be made separately from any other transaction or part of a transaction;

(ii) be made at least twenty-four hours after an individual creates an account or first uses the requested product or service;

(iii) be made in the absence of any mechanism that has the purpose or substantial effect of obscuring, subverting, or impairing an individual's decision-making regarding authorization for processing;

(iv) if requesting authorization for multiple categories of processing activities, allow the individual to provide/withhold authorization separately for each category of processing activity; and

(v) not include any request for authorization for a processing activity for which an individual has withheld or revoked authorization within the past calendar year.

(b) A valid authorization shall include:

(i) the types of regulated health information to be processed;

(ii) the nature of the processing activity;

(iii) the specific purposes for such processing;

(iv) the names where readily available, or categories of service providers and third parties to which the regulated entity may disclose the individual's regulated health information and the purposes for such disclosure, including the circumstances under which the regulated entity may disclose regulated health information to law enforcement;

(v) any monetary or other valuable consideration the regulated entity may receive in connection with processing the individual's regulated health information, where applicable;

(vi) that failing to provide authorization will not affect the individual's experience of using the regulated entity's products or services;

(vii) the expiration date of the authorization, which may be up to one year from the date authorization was provided;

(viii) the mechanism by which the individual may revoke authorization prior to expiration;

(ix) the mechanism by which the individual may request access to and deletion of their regulated health information;

(x) any other information material to an individual's decision-making regarding authorization for processing; and

(xi) the signature, which may be electronic, of the individual who is the subject of the regulated health information, or a parent or guardian authorized by law to take actions of legal consequence on behalf of the individual who is the subject of the regulated health information, and the date.

(c) (i) A regulated entity that receives authorization for processing shall provide an effective, efficient, and easy-to-use mechanism by which an individual may revoke authorization at any time through an interface regularly used in conjunction with the regulated entity's product or service.

(ii) Upon an individual's revocation of authorization, the regulated entity shall immediately cease all processing activities for which authorization was revoked, except to the extent necessary to comply with the regulated entity's legal obligations.

(iii) For individuals who have an online account with the regulated entity, the regulated entity must provide, in a conspicuous and easily accessible place within the account settings, a list of all processing activities for which the individual has provided authorization and, for each processing activity, allow the individual to revoke authorization in the same place with one motion or action.

(d) Upon obtaining valid authorization from an individual, the regulated entity shall provide that individual a copy of the authorization. The authorization shall be provided in a manner that is capable of being retained by the individual.

(e) The regulated entity shall limit its processing to what was clearly disclosed to an individual pursuant to paragraph (b) of this subdivi-

sion when the regulated entity received authorization from the individual.

(f) If the regulated entity seeks to materially alter its processing activities for regulated health information collected pursuant to authorization, the regulated entity shall obtain a new authorization for the new or altered processing activity.

(g) Providing a product or service requested by an individual must not be made contingent on providing authorization. The regulated entity must not discriminate against an individual for withholding authorization, such as by charging different prices or rates for products or services, including through the use of discounts or other benefits, imposing penalties, or providing a different level or quality of services or goods to the individual.

3. A regulated entity that processes regulated health information pursuant to a permissible purpose pursuant to subparagraph (ii) of paragraph (b) of subdivision one of this section shall comply with the following:

(a) A regulated entity shall provide clear and conspicuous notice that describes:

(i) the types of regulated health information to be processed;

(ii) the nature of the processing activity;

(iii) the specific purposes for such processing;

(iv) the names where readily available, or categories of service providers and third parties to which the regulated entity may disclose the individual's regulated health information and the purposes for such disclosure, including the circumstances under which the regulated entity may disclose regulated health information to law enforcement; and

(v) the mechanism by which the individual may request access to and deletion of their regulated health information.

(b) If the regulated entity materially alters its processing activities for regulated health information collected pursuant to a permissible purpose, the regulated entity must provide a clear and conspicuous notice in plain language, separate from a privacy policy, terms of service, or similar document, that describes any material changes to the processing activities and provide the individual with an opportunity to request deletion of their regulated health information.

§ 1103. Individual rights. 1. (a) A regulated entity shall make available an effective, efficient, and easy-to-use mechanism through an interface regularly used in conjunction with the regulated entity's product or service by which an individual may request access to their regulated health information.

(b) Within thirty days of receiving an access request, the regulated entity shall make available a copy of all regulated health information about the individual that the regulated entity maintains or that service providers maintain on behalf of the regulated entity.

2. (a) A regulated entity shall make available an effective, efficient, and easy-to-use mechanism through an interface regularly used in conjunction with the regulated entity's product or service by which an individual may request the deletion of their regulated health information.

(b) An individual's deletion or cancellation of their online account shall be treated as a request to delete the individual's regulated health information.

(c) Within thirty days of receiving a deletion request, the regulated entity shall:

(i) Delete all regulated health information associated with the individual in the regulated entity's possession or control, except to the extent necessary to comply with the regulated entity's legal obligations; and

(ii) Unless it proves impossible or involves disproportionate effort that is documented in writing by the regulated entity, communicate such request to each service provider or third party that processed the individual's regulated health information in connection with a transaction involving the regulated entity occuring within one year preceding the individual's request.

(d) Any service provider or third party that receives notice of an individual's deletion request shall within thirty days delete all regulated health information associated with the individual in its possession or control, except to the extent necessary to comply with its legal obligations.

3. Any right set forth in this section may be exercised at any time by the individual who is the subject of the regulated health information or an agent authorized by such individual.

§ 1104. Security. 1. In general, a regulated entity shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of regulated health information.

2. A regulated entity must securely dispose of an individual's regulated health information pursuant to a publicly available retention schedule within a reasonable time, and in no event later than sixty days, after it is no longer necessary to maintain for the permissible purpose or purposes identified in the notice or for which the individual provided valid authorization.

§ 1105. Service providers. 1. In general, any processing of regulated health information by a service provider on behalf of a regulated entity shall be governed by a written, binding agreement. Such agreement shall clearly set forth instructions for processing regulated health information, the nature and purpose of processing, the duration of processing, and the rights and obligations of both parties.

2. An agreement pursuant to subdivision one of this section shall require that the service provider:

(a) ensure that each person processing regulated health information is subject to a duty of confidentiality with respect to such information;

(b) protect regulated health information in a manner consistent with the requirements of this article;

(c) process regulated health information only when and to the extent necessary to comply with its obligations to the regulated entity;

(d) not combine the regulated health information which the service provider receives from or on behalf of the regulated entity with any other personal information which the service provider receives from or on behalf of another party or collects from its own relationship with individuals;

(e) comply with any exercises of an individual's rights under section eleven hundred three of this article upon the request of the regulated entity and notify any service providers or third parties to which it disclosed regulated health information of the request;

(f) delete or return all regulated health information to the regulated entity at the end of the provision of services, unless retention of the regulated health information is required by law;

(g) upon the reasonable request of the regulated entity, make available to the regulated entity all data in its possession necessary to

demonstrate the service provider's compliance with the obligations in this section;

(h) allow, and cooperate with, reasonable assessments by the regulated entity or the regulated entity's designated assessor for purposes of evaluating compliance with the obligations of this article; alternatively, the service provider may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this article using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The service provider shall provide a report of such assessment to the regulated entity upon request;

(i) a reasonable time in advance before disclosing or transferring regulated health information to any further service providers, notify the regulated entity of such a proposed disclosure or transfer, which may be in the form of a regularly updated list of further service providers that may access regulated health information; and

(j) engage any further service provider pursuant to a written, binding agreement that includes the contractual requirements provided in this section, containing at minimum the same obligations that the service provider has entered into with regard to regulated health information.

§ 1106. Exemptions. Nothing in this article shall apply to:

1. information processed by local, state, and federal governments, and municipal corporations;

2. protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5);

3. any covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the covered entity maintains patient information in the same manner as protected health information as described in subdivision two of this section;

4. information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration;

5. information processed pursuant to the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g) and its implementing regulations;

6. information processed pursuant to section two-d of the education law; and

7. information processed pursuant to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq).

§ 1107. Enforcement. 1. Whenever it appears to the attorney general, either upon complaint or otherwise, that any person or persons, within or outside the state, has engaged in or is about to engage in any of the

acts or practices stated to be unlawful under this article, the attorney general may bring an action or special proceeding in the name and on behalf of the people of the state of New York to enjoin any violation of this article, to obtain restitution of any moneys or property obtained directly or indirectly by any such violation, to obtain disgorgement of any profits obtained directly or indirectly by any such violation, to obtain civil penalties of not more than fifteen thousand dollars per violation or twenty percent of revenue obtained from New York consumers within the past fiscal year, whichever is greater, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

2. The remedies provided by this section shall be in addition to any other lawful remedy available.

3. Any action or special proceeding brought by the attorney general pursuant to this section must be commenced within six years of the date on which the attorney general became aware of the violation.

4. In connection with any proposed action or special proceeding under this section, the attorney general is authorized to take proof and make a determination of the relevant facts, and to issue subpoenas in accordance with the civil practice law and rules. The attorney general may also require such other data and information as he or she may deem relevant and may require written responses to questions under oath. Such power of subpoena and examination shall not abate or terminate by reason of any action or special proceeding brought by the attorney general under this article.

5. This section shall apply to all acts declared to be unlawful in this article, whether or not subject to any other law of this state, and shall not supersede, amend or repeal any other law of this state under which the attorney general is authorized to take any action or conduct any inquiry.

6. The attorney general may promulgate such rules and regulations as are necessary to effectuate and enforce the provisions of this section.

§ 2. Severability. If any clause, sentence, paragraph, subdivision, section or part of this act shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, section or part thereof directly involved in the controversy in which such judgment shall have been rendered. 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.

§ 3. This act shall take effect July 1, 2024.