STATE OF NEW YORK

3285

2023-2024 Regular Sessions

IN ASSEMBLY

February 2, 2023

Introduced by M. of A. L. ROSENTHAL, GALLAGHER, KELLES, SIMON, OTIS -- read once and referred to the Committee on Consumer Affairs and Protection

AN ACT to amend the general business law, in relation to electronic health products and services

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:

ARTICLE 42
ELECTRONIC HEALTH PRODUCTS AND SERVICES

Section 1100. Definitions.
1101. Electronic health products and services; privacy.
1102. Private right of action.
1103. Actions that are HIPAA compliant.

§ 1100. Definitions. For the purposes of this article, the following terms shall have the following meanings:

1. "Consent" means an action which (a) clearly and conspicuously communicates the individual's authorization of an act or practice; (b) is made in the absence of any mechanism in the user interface that has the purpose or substantial effect of obscuring, subverting, or impairing decision making or choice to obtain consent; and (c) cannot be inferred from inaction.

2. "Deactivation" means a user's deletion, removal, or other action made to terminate their use of an electronic health product or service.

3. "Electronic health product or service" means any software or hardware, including a mobile application, website, or other related product or service, that is designed to maintain personal health information, in order to make such personal health information available to a user or to a health care provider at the request of such user or health care

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

LBD01394-02-3

provider, for the purposes of allowing such user to manage their information, or for the diagnosis, treatment, or management of a medical condition.

4. "Health care provider" means:

(a) a hospital as defined in article twenty-eight of the public health law, a home care services agency as defined in article thirty-six of the public health law, a hospice as defined in article forty of the public health law, a health maintenance organization as defined in article forty-four of the public health law, or a shared health facility as defined in article forty-seven of the public health law; or

(b) a person licensed under article one hundred thirty-one, one hundred thirty-one-B, one hundred thirty-two, one hundred thirty-three, one hundred thirty-six, one hundred thirty-nine, one hundred forty-one, one hundred forty-three, one hundred forty-four, one hundred fifty-three, one hundred fifty-four, one hundred fifty-six or one hundred fifty-nine of the education law.

5. "Individually identifiable information" means any information that identifies or could reasonably be linked, directly or indirectly, to a particular consumer, household, or consumer device.

6. "Personal health information" means any individually identifiable information about an individual's mental or physical condition provided by such individual, or otherwise gained or inferred from monitoring such individual's mental or physical condition.

7. "Other personal data" means any individually identifiable information about an individual provided by such individual, or otherwise gained or inferred from monitoring such individual, other than personal health information.

8. "User" means an individual who has downloaded or uses an electronic health product or service.

9. "Data processing" means any action or set of actions performed on or with personal information, including but not limited to collection, access, use, retention, sharing, monetizing, analysis, creation, generation, derivation, decision-making, recording, alternation, organization, structuring, storage, disclosure, transmission, sale, licensing, disposal, destruction, de-identifying, or other handling of personal information.

10. "Covered organization" means an entity that offers an electronic health product or service that is subject to the provisions of this article.

§ 1101. Electronic health products and services; privacy. 1. (a) It shall be unlawful for a covered organization to engage in data processing unless:

(i) the user to whom the information or data pertains has given affirmative express consent to such data processing; or

(ii) such data processing is strictly necessary and proportionate for the purpose of:

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

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

(C) the covered organization is compelled to do so by a warrant or court order.

(b) The general nature of any data processing shall be conveyed by the covered organization in a standalone document such as a data processing addendum, and in clear and prominent terms in such a way that an ordinary consumer would notice and understand such terms.

(c) A user may consent to data processing on behalf of their dependent minors.

(d) A covered organization shall provide an effective mechanism for a user to revoke their consent after it is given. After a user revokes their consent, the covered organization shall cease all data processing of such user's personal health information or other personal data as soon as practicable, but not later than fifteen days after such user revokes such consent. The covered organization shall also delete or otherwise destroy any such user's personal health information or other personal data per the terms of paragraph (a) of subdivision four of this section.

2. In order to obtain consent in compliance with subdivision one of this section, an entity offering an electronic health product or service shall:

(a) disclose to the user all personal health information or other personal data such electronic health product or service will collect from the user upon obtaining consent;

(b) disclose to the user any third party with whom such user's personal health information or other personal data may be shared by the electronic health product or service upon obtaining consent;

(c) disclose to the user the purpose for collecting any personal health information or other personal data; and

(d) allow the user to withdraw consent at any time.

3. No electronic health product or service shall collect any personal health information or other personal data beyond which a user has specifically consented to share with such electronic health product or service under subdivision one of this section.

4. (a) An electronic health product or service shall delete or otherwise destroy any personal health information or other personal data collected from a user immediately upon such user's request, withdrawal of consent; or upon such user's deactivation of their account.

(b) An entity that collects a user's personal health information or other personal data shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a user has requested or is reasonably necessary for security or fraud prevention.

(c) An entity that collects a user's personal health information or other personal data shall limit its use and retention of such information to what is strictly necessary to provide a service or conduct an activity that a user has requested or a related operational purpose, provided that information collected or retained solely for security or fraud prevention may not be used for operational purposes. Monetization of personal health information or other personal data, including but not limited to the use of targeted advertising, cross-context behavioral advertising or marketing services, or the use of personal health information for training or inclusion in machine learning models, beyond that which a user has explicitly consented to shall not be considered strictly necessary to provide a service or conduct an activity or a related operational purpose.

(d) If a user deletes their personal health information or other personal data collected by an entity, or requests the entity delete their personal health information or other personal data, such entity shall retain such user's personal health information or other personal data on any server or data management system no longer than thirty days after such deletion or request. The entity must give the user an oppor-

tunity to download a copy of such personal health information or personal data prior to permanent deletion.

5. A covered organization shall not discriminate against a user because the user exercised any of the user's rights under this article, or did not agree to information processing for a separate product or service, including, but not limited to, by:

(a) Denying goods or services to the user.

(b) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(c) Providing a different level or quality of goods or services to the user.

(d) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

6. A covered organization shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the information and the purposes for which the personal health information or other personal data will be used, to protect consumers' personal health information or other personal data from unauthorized use, disclosure, access, destruction, or modification.

§ 1102. Private right of action. 1. Any person who has been injured by reason of a violation of this article may bring an action in their own name, or in the name of their minor child, to enjoin such unlawful act, or to recover the greater of their actual damages or one thousand dollars, or both such actions. The court shall award reasonable attorney's fees to a prevailing plaintiff. Actions pursuant to this section may be brought on a class-wide basis.

2. Any entity who violates this article is subject to an injunction and liable for damages and a civil penalty. When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the size and revenues of the covered entity. Each individual whose data was unlawfully processed counts as a separate violation. Each provision of this article that was violated counts as a separate violation.

§ 1103. Actions that are HIPAA compliant. Nothing in this article shall prohibit any action taken with respect to the health information of an individual by a business associate or covered organization that is permissible under the federal regulations concerning standards for privacy of individually identifiable health information promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996.

§ 2. This act shall take effect on the sixtieth day after it shall have become a law.