

STATE OF NEW YORK

158

2023-2024 Regular Sessions

IN SENATE

(Prefiled)

January 4, 2023

Introduced by Sen. KRUEGER -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the general business law, in relation to privacy standards for electronic health products and services and permissible data brokering

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 voluntary 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. A request for consent shall be provided to the individual in a clear and conspicuous disclosure, apart from any privacy policy, terms of service, terms of use, general release, user agreement, or other similar document, of all information material to the provision of consent.

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

LBD01105-01-3

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

4 3. "Electronic health product or service" means any software or hard-
5 ware, including a mobile application, website, or other related product
6 or service, that is designed to maintain personal health information,
7 designed to diagnose or designed to infer a medical diagnosis, in order
8 to make such personal health information available to a user or to a
9 health care provider at the request of such user or health care provid-
10 er, for the purposes of allowing such user to manage his or her informa-
11 tion, or for the diagnosis, inferred diagnosis, treatment, or management
12 of a medical condition.

13 4. "Health care provider" means:

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

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

26 5. "Personal health information" means any individually identifiable
27 information about an individual's mental or physical condition provided
28 by such individual, or otherwise gained from monitoring such individ-
29 ual's mental or physical condition.

30 6. "User" means an individual who has downloaded or uses an electronic
31 health product or service.

32 7. "Consumer data" means any information that identifies, relates to,
33 describes, is capable of being associated with, or could reasonably be
34 linked, either directly or indirectly, with a particular consumer
35 regardless if such data can be derived by the consumer, household, or
36 consumer device or derived from other sources such as an internet proto-
37 col address.

38 8. "Data processing" means the collection, use, disclosure, retention,
39 or processing of personal health information or other data.

40 9. "Covered organization" means an entity, including a data broker,
41 that offers an electronic health product or service that is subject to
42 the provisions of this article.

43 10. "Data broker" means a person or entity that collects, buys,
44 licenses, or infers data about individuals and then sells, licenses, or
45 trades that data.

46 11. "Digital advertiser" means any person, corporation, partnership or
47 association that delivers digital advertisements by electronic means.

48 12. "Digital advertisement" shall include any communication delivered
49 by electronic means that is intended to be used for the purposes of
50 marketing, solicitation, or dissemination of information related,
51 directly or indirectly, to goods or services provided by the digital
52 advertiser or a third party.

53 13. "Geofencing" means a technology that uses global positioning
54 system coordinates, cell tower connectivity, cellular data, radio
55 frequency identification, Wi-Fi data and/or any other form of location
56 detection, to establish a virtual boundary or "geofence" around a

particular location that allows a digital advertiser to track the location of an individual user and electronically deliver targeted digital advertisements directly to such user's mobile device upon such user's entry into the geofenced area.

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

(i) the user to whom the information or data pertains has given affirmative express consent to such data processing and if such covered organization will broker user data, the user must also give separate affirmative consent to such data brokering; and

(ii) such data processing, geofencing or data brokering, is strictly necessary and for the purpose of:

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

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

(C) complying with a court order issued to the covered organization.

(b) The general nature of any data processing or data brokering shall be conveyed by the covered organization 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 or data brokering on behalf of his or her 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 and data brokering of such user's personal health information or other data as soon as practicable, but not later than fifteen days after such user revokes such consent.

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

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

(b) disclose to the user all third parties 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 his or her account.

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

(c) A covered organization that collects a user's personal health information or other data shall limit its use and retention of such

1 information to what is reasonably necessary to provide a service or
2 conduct an activity that a user has requested or a related operational
3 purpose, provided that information collected or retained solely for
4 security or fraud prevention may not be used for operational purposes.

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

9 (a) Denying goods or services to the user.

10 (b) Charging different prices or rates for goods or services, includ-
11 ing through the use of discounts or other benefits or imposing penal-
12 ties.

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

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

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

25 7. (a) It shall be unlawful for any person, corporation, partnership
26 or association to deliver by electronic means any digital advertisement
27 to a user through the use of geofencing at any health care facility as
28 defined in subdivision one of this section.

29 (b) It shall be unlawful for any person, corporation, partnership or
30 association to establish a geofence or similar virtual boundary in or
31 around any health care facility for the purpose of delivering by elec-
32 tronic means a digital advertisement to a user within such health care
33 facility.

34 § 1102. Private right of action. 1. Any person who has been injured by
35 reason of a violation of this article may bring an action in his or her
36 own name, or in the name of his or her minor child, to seek declaratory
37 relief, to enjoin such unlawful act, to recover his or her actual
38 damages, to seek statutory damages as provided pursuant to this section,
39 or any combination of such actions. Any violation of this article
40 constitutes an injury-in-fact and a harm to any affected individual. The
41 court shall award reasonable attorney's fees to a prevailing plaintiff.

42 2. Any covered organization that violates this article is subject to
43 declaratory judgment, an injunction and liable for damages and a civil
44 penalty. When calculating damages and civil penalties, the court shall
45 consider the number of affected individuals, the severity of the
46 violation, and the size and revenues of the covered organization. Addi-
47 tionally, statutory damages shall be awarded in the amount of five
48 hundred dollars per violation. Each individual whose data was unlawfully
49 processed counts as a separate violation. Each provision of this article
50 that was violated counts as a separate violation.

51 § 1103. Actions that are HIPAA compliant. Nothing in this article
52 shall prohibit any action taken with respect to the health information
53 of an individual by a data broker that is a business associate or
54 covered organization that is permissible under the federal regulations
55 concerning standards for privacy of individually identifiable health

information promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d- 20 2 note).

§ 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 on the sixtieth day after it shall have become a law.