

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 Assem-
bly, do enact as follows:

1 Section 1. The general business law is amended by adding a new article
2 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.

3 § 1100. Definitions. For the purposes of this article, the following
4 terms shall have the following meanings:

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

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

13 3. "Electronic health product or service" means any software or hard-
14 ware, including a mobile application, website, or other related product
15 or service, that is designed to maintain personal health information, in
16 order to make such personal health information available to a user or to
17 a health care provider at the request of such user or health care
18

19
20
21
22
23
EXPLANATION--Matter in italics (underscored) is new; matter in brackets
[-] is old law to be omitted.

LBD01394-02-3

1 provider, for the purposes of allowing such user to manage their infor-
2 mation, or for the diagnosis, treatment, or management of a medical
3 condition.

4 4. "Health care provider" means:

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

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

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

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

24 7. "Other personal data" means any individually identifiable informa-
25 tion about an individual provided by such individual, or otherwise
26 gained or inferred from monitoring such individual, other than personal
27 health information.

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

30 9. "Data processing" means any action or set of actions performed on
31 or with personal information, including but not limited to collection,
32 access, use, retention, sharing, monetizing, analysis, creation, gener-
33 ation, derivation, decision-making, recording, alternation, organiza-
34 tion, structuring, storage, disclosure, transmission, sale, licensing,
35 disposal, destruction, de-identifying, or other handling of personal
36 information.

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

40 § 1101. Electronic health products and services; privacy. 1. (a) It
41 shall be unlawful for a covered organization to engage in data process-
42 ing unless:

43 (i) the user to whom the information or data pertains has given affir-
44 mative express consent to such data processing; or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23 § 1102. Private right of action. 1. Any person who has been injured by
24 reason of a violation of this article may bring an action in their own
25 name, or in the name of their minor child, to enjoin such unlawful act,
26 or to recover the greater of their actual damages or one thousand
27 dollars, or both such actions. The court shall award reasonable attor-
28 ney's fees to a prevailing plaintiff. Actions pursuant to this section
29 may be brought on a class-wide basis.

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

37 § 1103. Actions that are HIPAA compliant. Nothing in this article
38 shall prohibit any action taken with respect to the health information
39 of an individual by a business associate or covered organization that is
40 permissible under the federal regulations concerning standards for
41 privacy of individually identifiable health information promulgated
42 under section 264(c) of the Health Insurance Portability and Account-
43 ability Act of 1996.

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