STATE OF NEW YORK

6656

2021-2022 Regular Sessions

IN ASSEMBLY

March 23, 2021

Introduced by M. of A. L. ROSENTHAL -- 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:
 <u>ARTICLE 42</u>

ELECTRONIC HEALTH PRODUCTS AND SERVICES

5 <u>Section 1100. Definitions.</u>

4

б

7

1101. Electronic health products and services; privacy.

<u>1102. Private right of action.</u>

8 <u>§ 1100. Definitions. For the purposes of this article, the following</u>
9 terms shall have the following meanings:

10 1. "Consent" means an action which (a) clearly and conspicuously 11 communicates the individual's authorization of an act or practice; (b) 12 is made in the absence of any mechanism in the user interface that has 13 the purpose or substantial effect of obscuring, subverting, or impairing 14 decision making or choice to obtain consent; and (c) cannot be inferred 15 from inaction.

16 <u>2. "Deactivation" means a user's deletion, removal, or other action</u> 17 <u>made to terminate his or her use of an electronic health product or</u> 18 <u>service.</u>

19 3. "Electronic health product or service" means any software or hard-20 ware, including a mobile application, website, or other related product 21 or service, that is designed to maintain personal health information, in 22 order to make such personal health information available to a user or to 23 a health care provider at the request of such user or health care

23 <u>a health care provider at the request of such user or health care</u> 24 <u>provider, for the purposes of allowing such user to manage his or her</u>

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

LBD10359-01-1

A. 6656

1	information, or for the diagnosis, treatment, or management of a medical
2	condition.
3	4. "Health care provider" means:
4	(a) a hospital as defined in article twenty-eight of the public health
5	law, a home care services agency as defined in article thirty-six of the
6	public health law, a hospice as defined in article forty of the public
7	health law, a health maintenance organization as defined in article
8	forty-four of the public health law, or a shared health facility as
9	<u>defined in article forty-seven of the public health law; or</u>
10	(b) a person licensed under article one hundred thirty-one, one
11	hundred thirty-one-B, one hundred thirty-two, one hundred thirty-three,
12	one hundred thirty-six, one hundred thirty-nine, one hundred forty-one,
13	one hundred forty-three, one hundred forty-four, one hundred fifty-
14	three, one hundred fifty-four, one hundred fifty-six or one hundred
15	fifty-nine of the education law.
16	5. "Individually identifiable information" means any information that
17	identifies or could reasonably be linked, directly or indirectly, to a
18	particular consumer, household, or consumer device.
19	6. "Personal health information" means any individually identifiable
20	information about an individual's mental or physical condition provided by such individual, or otherwise gained from monitoring such individ-
21 22	ual's mental or physical condition.
22 23	7. "Other personal data" means any individually identifiable informa-
24	tion about an individual provided by such individual, or otherwise
25	gained from monitoring such individual, other than personal health
26	information.
27	8. "User" means an individual who has downloaded or uses an electronic
28	health product or service.
29	9. "Data processing" means the collection, use, disclosure, or proc-
30	essing of personal health information or other data.
31	10. "Covered organization" means an entity that offers an electronic
32	health product or service that is subject to the provisions of this
33	<u>article.</u>
34	§ 1101. Electronic health products and services; privacy. 1. (a) It
35	shall be unlawful for a covered organization to engage in data process-
36	ing unless:
37	(i) the user to whom the information or data pertains has given affir-
38	mative express consent to such data processing; and
39	(ii) such data processing is necessary and for the purpose of:
40	(A) protecting against malicious, deceptive, fraudulent, or illegal
41 42	<u>activity;</u> (B) detecting, responding to, or preventing security incidents or
42 43	threats; or
43 44	(C) the covered organization is compelled to do so by a legal obli-
45	gation.
46	(b) The general nature of any data processing shall be conveyed by the
47	covered organization in clear and prominent terms in such a way that an
48	ordinary consumer would notice and understand such terms.
49	(c) A user may consent to data processing on behalf of his or her
50	dependent minors.
51	(d) A covered organization shall provide an effective mechanism for a
52	user to revoke their consent after it is given. After a user revokes
53	their consent, the covered organization shall cease all data processing
54	of such user's personal health information or other data as soon as
55	practicable, but not later than fifteen days after such user revokes
56	such consent.

A. 6656

1	2. In order to obtain consent in compliance with subdivision one of
2	this section, an entity offering an electronic health product or service
3	shall:
4	(a) disclose to the user all personal health information or other
5	personal data such electronic health product or service will collect
6	from the user upon obtaining consent;
7	(b) disclose to the user any third party with whom such user's
8	personal health information or other personal data may be shared by the
9	electronic health product or service upon obtaining consent;
10	(c) disclose to the user the purpose for collecting any personal
11	health information or other personal data; and
12	(d) allow the user to withdraw consent at any time.
13	3. No electronic health product or service shall collect any personal
14	health information or other personal data beyond which a user has
15	specifically consented to share with such electronic health product or
16	service under subdivision one of this section.
17	4. (a) An electronic health product or service shall delete or other-
18	wise destroy any personal health information or other personal data
19	collected from a user immediately upon such user's request, withdrawal
20	of consent; or upon such user's deactivation of his or her account.
21	(b) An entity that collects a user's personal health information or
22	other data shall limit its collection and sharing of that information
23	with third parties to what is reasonably necessary to provide a service
24	
	or conduct an activity that a user has requested or is reasonably neces-
25	sary for security or fraud prevention. Monetization of information or
26	data shall be considered reasonably necessary to provide a service or
27	conduct an activity that a user has requested or reasonably necessary
28	for security or fraud prevention.
29	(c) An entity that collects a user's personal health information or
30	other data shall limit its use and retention of such information to what
31	is reasonably necessary to provide a service or conduct an activity that
32	a user has requested or a related operational purpose, provided that
33	information collected or retained solely for security or fraud
34	prevention may not be used for operational purposes.
35	5. A covered organization shall not discriminate against a user
36	because the user exercised any of the user's rights under this title, or
37	did not agree to information processing for a separate product or
38	service, including, but not limited to, by:
39	(a) Denying goods or services to the user.
40	(b) Charging different prices or rates for goods or services, includ-
41	ing through the use of discounts or other benefits or imposing penal-
42	ties.
43	(c) Providing a different level or quality of goods or services to the
44	<u>user.</u>
45	(d) Suggesting that the consumer will receive a different price or
46	rate for goods or services or a different level or quality of goods or
47	services.
48	6. A covered organization shall implement and maintain reasonable
	security procedures and practices, including administrative, physical,
49 50	
50	and technical safeguards, appropriate to the nature of the information
51	and the purposes for which the personal health information or other data
52	will be used, to protect consumers' personal health information or other
53	data from unauthorized use, disclosure, access, destruction, or modifi-
54	cation.
55	§ 1102. Private right of action. 1. Any person who has been injured by
56	reason of a violation of this article may bring an action in his or her

A. 6656

1	own name, or in the name of his or her minor child, to enjoin such
2	unlawful act, or to recover his or her actual damages, or both such
3	actions. The court may award reasonable attorney's fees to a prevailing
4	<u>plaintiff.</u>
5	2. Any entity who violates this article is subject to an injunction
б	and liable for damages and a civil penalty. When calculating damages and
7	civil penalties, the court shall consider the number of affected indi-
8	viduals, the severity of the violation, and the size and revenues of the
9	covered entity. Each individual whose data was unlawfully processed
10	counts as a separate violation. Each provision of this article that was
11	violated counts as a separate violation.
12	§ 2. This act shall take effect on the sixtieth day after it shall
13	have become a law.