

STATE OF NEW YORK

8448--B

IN SENATE

June 3, 2020

Introduced by Sen. THOMAS -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT in relation to the collection of emergency health data and the use of technology to aid during COVID-19; and providing for the repeal of such provision upon the expiration thereof

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

- 1 Section 1. For the purposes of this act:
- 2 1. "Covered entity" means any person, including a government entity:
- 3 (a) that collects, uses, or discloses emergency health data, as
- 4 defined in this act, electronically or through communication by wire or
- 5 radio; or
- 6 (b) that develops or operates a website, web application, mobile
- 7 application, mobile operating system feature, or smart device applica-
- 8 tion for the purpose of tracking, screening, monitoring, contact trac-
- 9 ing, or mitigation, or otherwise responding to the COVID-19 public
- 10 health emergency.
- 11 2. "De-identified information" means information that cannot reason-
- 12 ably identify, relate to, describe, be capable of being associated with,
- 13 or be linked, directly or indirectly, to a particular individual, house-
- 14 hold, or device. A covered entity that uses de-identified information:
- 15 (a) has implemented technical safeguards that prohibit re-identifica-
- 16 tion of the individual to whom the information may pertain;
- 17 (b) has implemented business processes that specifically prohibit
- 18 re-identification of the information;
- 19 (c) has implemented business processes that prevent inadvertent
- 20 release of de-identified information; and
- 21 (d) makes no attempt to re-identify the information.
- 22 3. "Emergency health data" means data linked or reasonably linkable to
- 23 an individual or device, including data inferred or derived about the
- 24 individual, household, or device from other collected data provided such

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

LBD16478-04-0

1 data is still linked or reasonably linkable to the individual, house-
2 hold, or device, that concerns the public COVID-19 health emergency.
3 Such data includes:

4 (a) Information that reveals the past, present, or future physical or
5 behavioral health or condition of, or provision of healthcare to, an
6 individual including:

7 (i) data derived from the testing or examination;

8 (ii) whether or not an individual has contracted or been tested for,
9 or an estimate of the likelihood that a particular individual may
10 contract, such disease or disorder; and

11 (iii) genetic data, biological samples and biometrics; and

12 (b) Other data collected in conjunction with other emergency health
13 data that can be used to infer health status, health history, location
14 or associations, including:

15 (i) geolocation data, when such term means data capable of determining
16 the past or present precise physical location of an individual at a
17 specific point in time, taking account of population densities, includ-
18 ing cell-site location information, triangulation data derived from
19 nearby wireless or radio frequency networks and global positioning
20 system data;

21 (ii) proximity data, when such term means information that identifies
22 or estimates the past or present physical proximity of one individual or
23 device to another, including information derived from Bluetooth, audio
24 signatures, nearby wireless networks, and near field communications;

25 (iii) demographic data;

26 (iv) contact information for identifiable individuals or a history of
27 the individual's contacts over a period of time, such as an address book
28 or call log; and

29 (v) any other data collected from a personal device.

30 4. "Individual" means a natural person whom the covered entity knows
31 or has reason to know is located in New York state.

32 5. "Personal information" means information that identifies, relates
33 to, describes, is capable of being associated with, or could reasonably
34 be linked, directly or indirectly, with a particular individual or
35 household, or device.

36 6. "Process" means any operation or set of operations that are
37 performed on personal data by either automated or not automated means.

38 7. "Public health authority" means the New York state department of
39 health, a county health department or the New York city department of
40 health and mental hygiene, or a person or entity acting under a grant of
41 authority from or contract with such public agency, including the
42 employees or agents of such public agency or its contractors or persons
43 to entities to whom it has granted authority, that is responsible for
44 public health matters as part of its official mandate.

45 § 2. All covered entities must disclose the following information at a
46 fourth grade reading level or below and in the language the entity regu-
47 larly uses to communicate with the individual:

48 1. The individual's right to opt-in. (a) A covered entity shall obtain
49 freely given, specific, informed, and unambiguous opt-in consent from an
50 individual to:

51 (i) process the individual's personal information or emergency health
52 data; and

53 (ii) make any changes in the processing of the individual's personal
54 information or emergency health data.

55 (b) It shall be unlawful for a covered entity to collect, use, or
56 disclose emergency health data unless:

(i) the individual to whom the data pertains has freely given, specific, informed, and unambiguous consent to such collection, use, or disclosure; or

(ii) such collection, use, or disclosure is necessary and for the sole purpose of:

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

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

(c) To the extent that a covered entity must process internet protocol addresses, system configuration information, URLs of referring pages, locale and language preferences, keystrokes, and other personal information in order to obtain individuals' freely given, specific, informed, and unambiguous opt-in consent, the entity:

(i) shall only process the personal information necessary to request freely given, specific, informed, and unambiguous opt-in consent;

(ii) shall process the personal information solely to request freely given, specific, informed, and unambiguous opt-in consent; and

(iii) shall immediately delete the personal information if consent is withheld or withdrawn.

2. The individual's right to privacy. (a) All emergency health data and personal information shall be collected at a minimum level of identifiability reasonably needed for tracking COVID-19. For a covered entity using proximity tracing or exposure notification this includes changing temporary anonymous identifiers at least once in a 10 minute period.

(b) A covered entity shall not process personal information beyond what is adequate, relevant, and necessary for the completion of the transaction disclosed to, affirmatively consented to, and requested by the individual.

(c) A covered entity shall not process emergency health data for any purpose not authorized under this act, including:

(i) commercial advertising, recommendation for e-commerce, or the training of machine learning algorithms related to, or subsequently for use in, commercial advertising and e-commerce;

(ii) soliciting, offering, selling, leasing, licensing, renting, advertising, marketing, or otherwise commercially contracting for employment, finance, credit, insurance, housing, or education; or

(iii) segregating, discriminating in, or otherwise making unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation (as such term is defined in section 301 of the Americans with Disabilities Act of 1990), except as authorized by a state or federal government entity for a public health purpose.

3. Covered entity privacy policy. (a) A covered entity shall provide to the individual a privacy policy, prior to or at the point of collection of emergency health data:

(i) detailing how and for what purpose the covered entity collects, uses, and discloses emergency health data;

(ii) describing the covered entity's data retention and data security policies and practices for emergency health data; and

(iii) describing how an individual may exercise rights under this section.

(b) A covered entity shall create transparency reports, at least once every 90 days, that include:

(i) the number of individuals whose emergency health data the covered entity collected or used;

1 (ii) the categories of emergency health data collected, used, or
2 disclosed;

3 (iii) the purposes for which each category of emergency health data
4 was collected, used, or disclosed;

5 (iv) the number of requests for individuals emergency health data,
6 including information on who the emergency health data was disclosed to;
7 and

8 (v) the number of instances where emergency health data was produced,
9 in whole or in part, without prior, explicit consents by the individuals
10 specified in the request.

11 4. Time limitation on retention. (a) Emergency health data and
12 personal information shall be deleted when the initial purpose for
13 collecting or obtaining such data has been satisfied or within 30 days,
14 whichever occurs first, except that proximity tracing or exposure
15 notification data which shall be automatically deleted every 14 days.

16 (b) This subdivision shall not apply to de-identified information.

17 5. Access rights. (a) Emergency health data shall be disclosed only as
18 necessary to provide the service requested by an individual.

19 (b) A covered entity may share aggregate, de-identified data with
20 public health authorities.

21 (c) A covered entity shall not disclose emergency health data to a
22 third party unless that third party is contractually bound to the
23 covered entity to meet the same privacy and security obligations as the
24 covered entity.

25 (d) No covered entity in possession of emergency health data may
26 disclose, redisclose, or otherwise disseminate an individual's emergency
27 health data unless the subject of the personal information or the
28 subject's legally authorized representative consents in writing to the
29 disclosure or redisclosure.

30 (e) Individuals shall have the right to access the emergency health
31 data collected on them and correct any inaccuracies.

32 (i) A covered entity must comply with an individual's request to
33 correct emergency health data not later than 30 days after receiving a
34 verifiable request from the individual or, in the case of a minor, the
35 individual's parent or guardian.

36 (ii) Where the covered entity has reasonable doubts or cannot verify
37 the identity of the individual making a request under this paragraph,
38 the covered entity may request additional information necessary for the
39 specific purpose of confirming the identity of the individual. In such
40 cases, the additional information shall not be processed for any purpose
41 other than verifying the identity of the individual and must be deleted
42 immediately upon verification or failure to verify the individual.

43 § 3. 1. A covered entity shall implement reasonable measures to ensure
44 confidentiality, integrity, and availability of emergency health data
45 and personal information.

46 2. A covered entity that collects an individual's emergency health
47 data shall implement and maintain reasonable security procedures and
48 practices, including administrative, physical, and technical safeguards,
49 appropriate to the nature of the information and the purposes for which
50 that information will be used, to protect that information from unau-
51 thorized use, disclosure, access, destruction, or modification.

52 3. A covered entity shall limit access to emergency health data to
53 authorized essential personnel whose use of the data is reasonably
54 necessary to operate the program and record who has accessed emergency
55 health data, the date of access, and for what purposes.

§ 4. 1. All covered entities shall be subject to data protection audits, conducted by a neutral third party auditor, evaluating the technology utilized and the development processes for statistical impacts on classes protected under section 296 of article 15 of the executive law, as well as for impacts on privacy, and security that includes at a minimum:

(a) a detailed description of the technology, its design, and its purpose;

(b) an assessment of the relative benefits and costs of the technology in light of its purpose, taking into account relevant factors including data minimization practices; the duration for which personal information and the results of the data analysis are stored; what information about the technology is available to the public; and the recipients of the results of the technology;

(c) an assessment of the risk of harm posed by the technology; the risk that the technology may result in or contribute to inaccurate, unfair, biased, or discriminatory decisions; the risk that the technology may dissuade New Yorkers from participating in contact tracing or obtaining medical testing or treatment; and the risk that personal information or emergency health data can be accessed by third parties, including, but not limited to law enforcement agencies and U.S. Immigration and Customs Enforcement; and

(d) the measures the covered entity will employ to minimize the risks described in paragraph (c) of this subdivision, including technological, legal and physical safeguards;

(e) an assessment of whether the covered entity has followed through on the promises made in its privacy notice regarding collection, access, sharing, retention, deletion and sunseting; and

(f) if the technology utilizes machine-learning systems, a description of the training data information.

2. The audits required by this subdivision shall be made fully available to the public.

§ 5. 1. Private right of action.

(a) Any individual alleging a violation of this act or a regulation promulgated under this act may bring a civil action in any court of competent jurisdiction.

(b) A violation of this act or a regulation promulgated under this act with respect to the personal information of an individual constitutes a rebuttable presumption of harm to that individual.

(c) In a civil action in which the plaintiff prevails, the court may award:

(i) liquidated damages of ten thousand dollars or actual damages, whichever is greater;

(ii) punitive damages; and

(iii) any other relief, including an injunction, that the court determines is appropriate.

(d) In addition to any relief awarded pursuant to paragraph (c) of this subdivision, the court shall award reasonable attorney's fees and costs to any prevailing plaintiff.

2. The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce the provisions of this act. In an action brought by the attorney general, the court may award injunctive relief, including preliminary injunctions, to prevent further violations of and compel compliance with this act; civil penalties up to twenty-five thousand dollars per violation or up to four percent of annual revenue; other appropriate

1 relief, including restitution, to redress harms to individuals or to
2 mitigate all substantial risk of harm; and any other relief the court
3 determines.
4 § 6. This act shall take effect on the thirtieth day after it shall
5 have become a law and shall expire and be deemed repealed January 1,
6 2023.