

STATE OF NEW YORK

10583

IN ASSEMBLY

June 4, 2020

Introduced by COMMITTEE ON RULES -- (at request of M. of A. L. Rosenthal) -- read once and referred to the Committee on Health

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:

Section 1. For the purposes of this act:

1. "Covered entity" means any person, including a government entity:

(a) that collects, uses, or discloses emergency health data, as defined in this act, electronically or through communication by wire or radio; or

(b) that develops or operates a website, web application, mobile application, mobile operating system feature, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency.

2. "De-identified information" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual. A covered entity that uses de-identified information:

(a) has implemented technical safeguards that prohibit re-identification of the individual to whom the information may pertain;

(b) has implemented business processes that specifically prohibit re-identification of the information;

(c) has implemented business processes that prevent inadvertent release of de-identified information; and

(d) makes no attempt to re-identify the information.

3. "Emergency health data" means data linked or reasonably linkable to an individual or device, including data inferred or derived about the individual or device from other collected data provided such data is still linked or reasonably linkable to the individual or device, that concerns the public COVID-19 health emergency. Such data includes:

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

LBD16478-02-0

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

(i) data derived from the testing or examination;

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

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

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

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

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

(iii) demographic data;

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

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

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

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

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

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

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

(i) process the individual's emergency health data; and

(ii) make any changes in the processing of the individual's emergency health data.

(b) It shall be unlawful for a covered entity to collect, use, or 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; or

(iii) the covered entity is compelled to do so by a court order or other legal obligation.

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

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

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

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

12 2. The individual's right to privacy. (a) All emergency health data
13 and personal information shall be collected at a minimum level of iden-
14 tifiability reasonably needed for tracking COVID-19. For a covered enti-
15 ty using proximity tracing or exposure notification this includes chang-
16 ing temporary anonymous identifiers at least once in a 10 minute period.

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

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

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

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

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

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

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

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

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

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

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

48 (ii) the categories of emergency health data collected, used, or
49 disclosed;

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

52 (iv) the number of requests for individuals emergency health data,
53 including information on who the emergency health data was disclosed to;
54 and

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

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

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

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

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

14 (c) A covered entity shall not disclose emergency health data to a
15 third party unless that third party is contractually bound to the
16 covered entity to meet the same privacy and security obligations as the
17 covered entity.

18 (d) No covered entity in possession of emergency health data may
19 disclose, redisclose, or otherwise disseminate an individual's emergency
20 health data unless:

21 (i) the subject of the personal information or the subject's legally
22 authorized representative consents in writing to the disclosure or
23 redisclosure; or

24 (ii) the disclosure or redisclosure is required by state or federal
25 law.

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

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

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

39 § 3. 1. A covered entity shall implement reasonable measures to ensure
40 confidentiality, integrity, and availability of emergency health data
41 and personal information.

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

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

52 § 4. 1. All covered entities shall be subject to data protection
53 audits evaluating the technology utilized and the development processes
54 for statistical impacts on classes protected under section 296 of arti-
55 cle 15 of the executive law, as well as for impacts on privacy, and
56 security that includes at a minimum:

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

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

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

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

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

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

25 2. The audits required by this subdivision shall be made fully avail-
26 able to the public.

27 § 5. 1. An individual may bring a private right of action in a court
28 of competent jurisdiction to enforce any right under this act or to
29 enjoin any violation of this act.

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

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

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

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

40 (ii) punitive damages; and

41 (iii) any other relief, including an injunction, that the court deter-
42 mines is appropriate.

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

46 2. The attorney general may bring an action in the name of the state,
47 or as *parens patriae* on behalf of persons residing in the state, to
48 enforce the provisions of this act. In an action brought by the attorney
49 general, the court may award injunctive relief, including preliminary
50 injunctions, to prevent further violations of and compel compliance with
51 this act; civil penalties up to twenty-five thousand dollars per
52 violation or up to four percent of annual revenue; other appropriate
53 relief, including restitution, to redress harms to individuals or to
54 mitigate all substantial risk of harm; and any other relief the court
55 determines.

1 § 6. This act shall take effect on the thirtieth day after it shall
2 have become a law and shall expire and be deemed repealed January 1,
3 2023.