STATE OF NEW YORK

8448--C

IN SENATE

June 3, 2020

Introduced by Sens. THOMAS, BAILEY, CARLUCCI, GOUNARDES, HOYLMAN, MAY, RAMOS, STAVISKY -- 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 -- 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 personal information 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. "Collect" means to buy, rent, gather, obtain, receive, or access any personal information pertaining to an individual by any means, online or offline, including but not limited to, receiving information from the individual or from a third party, actively or passively, or obtaining information by observing an individual's behavior.

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

(a) that collects, processes, 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.

3. "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, household, or device. A covered entity that uses de-identified information:

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

LBD16478-12-0

(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.
4. "Disclose" means any action, set of actions, or omission in which a covered entity makes personal information available to another person, intentionally or unintentionally, including but not limited to, sharing, publishing, releasing, transferring, disseminating, making available, selling, leasing, providing access to, failing to restrict access to, or otherwise communicating orally, in writing, electronically, or by any other means.
5. "Emergency health data" means data linked or reasonably linkable to an individual, household, or device, including data inferred or derived about the individual, household, or device from other collected data provided such data is still linked or reasonably linkable to the individual, household, or device, that concerns the public COVID-19 health emergency. Such data includes:
(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.
6. "Individual" means a natural person whom the covered entity knows or has reason to know is located in New York state.
7. "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.
8. "Process" means any operation or set of operations that are performed on personal data by either automated or not automated means.
9. "Public health authority" means the New York state department of health, a county health department or the New York city department of

health and mental hygiene, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons to entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

§ 2. Individual rights.

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 personal information or emergency health data; and

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

(b) It shall be unlawful for a covered entity to collect, process, or disclose emergency health data or personal information unless:

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

(ii) such collection, processing, 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 the completion of the transaction disclosed to, affirmatively consented to, and requested by the individual. For a covered entity using proximity tracing or exposure notification this includes changing temporary anonymous identifiers at least once in a 20 minute period.

(b) A covered entity shall not process personal information or emergency health data 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 or personal information 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; provided that a covered entity shall not process emergency health data or personal information to make categorical decisions about the allocation of care based on disability.

3. Covered entity privacy policy. (a) A covered entity shall provide to the individual a privacy policy, at a fourth grade reading level or below and in the language the entity regularly uses to communicate with the individual, prior to or at the point of collection of emergency health data or personal information:

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

(ii) describing the covered entity's data retention and data security policies and practices for emergency health data and personal information; 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 or personal information the covered entity collected or processed;

(ii) the categories of emergency health data and personal information collected, processed, or disclosed;

(iii) the purposes for which each category of emergency health data or personal information was collected, processed, or disclosed;

(iv) the number of requests for individuals' emergency health data or personal information, including information on who the emergency health data or personal information was disclosed to; and

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

(c) The covered entity shall make each transparency report persistently available and readily accessible on such entity's website.

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

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

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

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

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

(d) No covered entity in possession of emergency health data or personal information may disclose, redisclose, or otherwise disseminate an individual's emergency health data or personal information unless the subject of the emergency health data or personal information or the

subject's legally authorized representative consents in writing to the disclosure or redisclosure.

(e) Without consent under subdivision one of this section, emergency health data, personal information, and any evidence derived therefrom shall not be subject to or provided in response to any legal process or be admissible for any purpose in any judicial or administrative action or proceeding.

(f) Individuals shall have the right to access the emergency health data and personal information collected on them and correct any inaccuracies.

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

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

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

2. A covered entity that collects an individual's emergency health data or personal information shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the information and the purposes for which that information will be processed, to protect that information from unauthorized processing, disclosure, access, destruction, or modification.

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

§ 4. 1. All covered entities shall be subject to annual 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 emergency health data 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 sunsetting; and

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

2. The covered entity shall make the audit persistently available and readily accessible on such entity's website.

3. The cost of the audit shall be paid by the covered entity.

§ 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 relief, including restitution, to redress harms to individuals or to mitigate all substantial risk of harm; and any other relief the court determines.

§ 6. 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.

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