Model State Pandemic Digital Rights Protection Bill

Section 1. Short title. This Act may be cited as the Pandemic Digital Rights Act.

Section 2. Findings. The [Legislature] finds that:

(a) The state has begun to deploy or consider deploying location tracking methods, artificial intelligence, algorithms, facial recognition, and other Automated Decision Systems in response to the COVID-19 pandemic;

(b) Some of these systems can improve the public health response to the pandemic;

(c) Some of these systems are being developed or operated by private companies;

(d) These systems have broad, and sometimes unexpected, impacts on the privacy of health records, the fairness of criminal penalties, the eligibility of individuals to receive government benefits, and on both workplace and student privacy;

(e) Use of some of these systems poses an inherent risk of bias and inaccuracy;

(f) The state has not given the public adequate information about these systems;

(g) The state currently does not adequately regulate Automated Decision Systems or the management and retention of personal data.

Section 3. Definitions. – As used in this Act, the term:

(a) “Algorithm” means a specific procedure, set of rules, or order of operations designed to solve a problem or make a calculation, classification, or recommendation.

(b) “Automated Decision System” means any system that uses algorithms, machine learning, natural language processing or other artificial intelligence technique to make decisions or assist in decision making for the state or any subdivisions thereof related to a public health emergency.

(b) “Developer” means a person or entity that developed or contributed to the development of an Automated Decision System.

(c) “Emergency Health Data” means any data that is linked or reasonably linkable to an individual, household or device, including data inferred or derived about the individual or device from other collected data, which was collected in connection with the treatment of, diagnosis of, public health response to, or research into a public health emergency.

(d) “Affirmative Express Consent” means a deliberate interaction by an individual that clearly communicates the individual’s authorization for an act in response to a specific request. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's authorization to act.

(e) “Source Code” is the original programming instructions of a piece of software, written in the language chosen by the programmer(s). The source code is different than a description of the system and the “object code,” which is used to execute the software on a computer system.

(f) “Digital Contact Tracing System” means a computer system, such as a mobile phone application or other centralized computer system, to identify individuals who may have been exposed to a communicable disease to facilitate testing, quarantine, and treatment.

(g) “Automated Exposure Notification system” means a computer system, such as a smartphone application, used to identify and notify individuals who may have been exposed to a communicable disease to facilitate testing, quarantine, or treatment.

(h) “Independent validation study” is an evaluation, completed by an entity other than the one that developed the system, of the accuracy, efficacy, and any biases of an Automated Decision System.

(i) “Training data” means the data used to inform the development of any Automated Decision System.

Section 4. Transparency Requirements

(a) Any state or private entity, prior to operating an Automated Decision System or Automated Exposure Notification System in response to a public health emergency, must publish the following:

(1) The developer of the system;

(2) The purpose of the system;

(3) A stated evaluation of benefits and risks;

(4) The data collected and the purposes for which that data is collected;

(5) The storage sharing, maintenance, retention, and deletion policies;

(6) A procedure by which an individual can access the factors, the logic, and the techniques that were the basis of an automated decision about them;

(7) A procedure by which an individual can request human review of an automated decision made about them;

(8) An independent validation study of the system; and

(9) A cybersecurity risk and protection framework.

(b) Following the conclusion of the public health emergency, any state or private entity that operated a system described in 4(a) must:

(1) Publish an evaluation of the systems efficacy and compliance with the purposes and limitations described in (4)(a);

(2) Confirm that the entity has deleted the Emergency Health Data collected for the system.

Section 5. Minimum Privacy Requirements for Emergency Health Data

(a) Any state or private entity using a system described in (4)(a) shall:

(1) Obtain affirmative express consent from an individual before collecting, using, or maintaining their Emergency Health Data;

(2) Include clear and conspicuous opt-out notices and consumer friendly mechanisms to allow an individual to opt out of the collection, use, or maintenance of their Emergency Health Data at any time;

(3) Only collect, use, or disclose emergency health data that is necessary, proportionate, and limited for public health purposes;

(4) Deploy, where possible, privacy enhancing techniques such as deidentification;

(5) Delete the Emergency Health Data of participating individuals on a rolling basis within 30 days of receipt of such data;

(6) Retain audit logs tracking access, use, and transfer of all Emergency Health Data;

(7) Provide individuals with a mechanism to access, correct, and delete Emergency Health Data;

(8) Implement reasonable data security policies, practices, and procedures to protect emergency health data; and

(9) Encrypt Emergency Health Data and conduct routine security testing and audits pursuant to best practices developed by the National Institute of Standards and Technology.

(b) Public health authorities and private entities that collect Emergency Health Data shall only disclose emergency health data to a government entity when the disclosure is to a public health authority, made for public health purposes, and in response to exigent circumstances.

(c) State and private entities shall not discriminate against an individual based on their refusal or inability to disclose Emergency Health Data or participate in a system described in 4(a). This includes but is not limited to factoring in non-participation in future public benefit decisions, law enforcement programs, or voting rights.

Section 6. Rights for individuals aggrieved by violations of this bill

(a) Any person subject to data collection or otherwise using a system described in (4)(a) shall have the right to:

(1) Request deletion of their Emergency Health Data from any system;

(2) Access their Emergency Health Data and all audit logs associated with that data;

(3) Access the factors, the logic, and the techniques that were the basis of a determination about them using an Automated Decision System;

(4) Correct any errors in their Emergency Public Health data and to appeal any determination about them made using an Automated Decision System.

(b) The state Attorney General may bring a civil action on behalf of its residents to enforce violations of this law, including the monetary relief per violation and injunctive relief.

(c) Any person aggrieved by a violation of this Act shall have a right of action in a State court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) Against a private or public entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) Against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; and

(3) Reasonable attorneys' fees and costs.