Public Health Emergency Privacy Act
Section-by-Section Summary

Section 1 – Short Title: the **"**Public Health Emergency Privacy Act"

Section 2 – Definitions [*excerpts of key definitions, excluding full inclusions & exclusions*]

(1) Affirmative Express Consent – An affirmative act by an individual that (A) clearly and conspicuously communicates the individual's authorization of an act or practice; (B) is made in the absence of any mechanism in the user interface that has the purpose or substantial effect of obscuring, subverting, or impairing decision-making or choice to obtain consent; and (C) cannot be inferred from inaction.

(2) Covered Organization –

- Any person (including a government entity) that collects, uses, or discloses emergency health data electronically or through communication by wire or radio; or 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.
- Does not include a health care provider; a person engaged in a de minimis collection or processing of emergency health data; a service provider; a person acting in their individual or household capacity; a public health authority.

(10) Emergency Health Data – Data linked or reasonably linkable to an individual or device, including inferred data, that concerns the COVID-19 public health emergency.

(11) Public Health Authority - An entity that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions, as well as a person, designated agency or associate, or entity acting under a grant of authority from, or under a contract with, such public health agency, including the employees or agents of such public health agency or its contractors or persons or entities to whom it has granted authority.

(12) COVID-19 Public Health Emergency - The outbreak and health response pertaining to Coronavirus Disease 2019 (COVID-19) associated with the emergency declared by the Secretary on January 31, 2020 under section 319 of Public Health Service Act (42 U.S.C. 247d), and any renewals thereof or any subsequent declarations by the Secretary related to the coronavirus.

(16) Service Provider – A person that collects, uses, or discloses emergency health data for the sole purpose of, and only to the extent that such entity is, conducting business activities on behalf of, for the benefit of, under instruction of, and under contractual agreement with a covered

organization. Such person shall only be considered a service provider in the course of activities previously described. Excludes a person that develops or operates a website, web application, mobile application, or app for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency.

Section 3 – Protection of Privacy Related to Emergency Health Data

(a) RIGHT TO PRIVACY – A covered organization shall:

- Only collect, use, or disclose such data that is necessary, proportionate, and limited for a good faith public health purpose.
- Take reasonable measures to ensure the accuracy of emergency health data and provide a mechanism for an individual to correct inaccurate information.
- Adopt reasonable safeguards to prevent unlawful discrimination based.
- Only disclose to a government entity if (1) to a public health authority; or (2) solely for good faith public health purposes and in direct response to exigent circumstances.

(b) RIGHT TO SECURITY – A covered organization or service provider that collects, uses, or discloses emergency health data shall establish and implement reasonable data security policies, practices, and procedures to protect the security and confidentiality of emergency health data.

(c) PROHIBITED USES – A covered organization shall not collect, use, or disclose emergency health data for any purpose not authorized under this section, including

- ads, e-commerce, or the machine learning algorithm training for ads or e-commerce;
- soliciting, offering, selling, leasing, licensing, renting, advertising, marketing, or otherwise commercially contracting in civil rights contexts (e.g., employment, finance, credit, insurance, housing, or education) in a manner that discriminates on the basis of emergency health data; and
- segregating, discriminating, or otherwise making unavailable goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of emergency health data.

(d) CONSENT – It shall be unlawful for a covered organization to collect, use, or disclose emergency health data unless the individual to whom the data pertains has given affirmative express consent; or the collection is necessary for protecting against fraud or preventing information security incidents; or a legal obligation. Consent must be revocable.

(e) NOTICE – A covered organization shall provide a privacy policy that is disclosed in a clear and conspicuous manner prior to collection; describes purposes for collection, use, and disclosure; describes data retention and security policies; and describes the rights under this Act.

(f) PUBLIC REPORTING – A covered organization collecting data of at least 100,000 individuals must issue a public report at least every 90 days stating:

- the number of individuals whose data was collected, used, or disclosed; and

- the categories of emergency health data and purposes for which it was collected, used, or disclosed, and the categories of third parties to whom it was disclosed;

(g) REQUIRED DATA DESTRUCTION —Except as required by the Privacy Act of 1974, HIPAA, or federal or state medical records retention and health privacy laws, a covered organization may not use or maintain emergency health data of an individual after the later of—

- 60 days after the termination of the public health emergency declared by the Secretary on January 31, 2020 pertaining to Coronavirus Disease 2019 (COVID-19);
- 60 days after the termination of a public health emergency declared by a governor pertaining to Coronavirus Disease 2019 (COVID-19); or
- 60 days after collection.

(g) EMERGENCY DATA COLLECTED, USED, OR DISCLOSED BEFORE ENACTMENT – The FTC shall promulgate regulations to ensure a covered organization that collected, used, or disclosed emergency health data before this Act are in compliance with this Act, to the degree practicable. The FTC shall initiate the rulemaking within 7 days and complete it within 45 days.

(h) NON-APPLICATION TO MANUAL CONTACT TRACING AND CASE INVESTIGATION – This Act does not limit or prohibit a public health authority from administering programs or activities to identify individuals who have contracted, or may have been exposed to, COVID-19 through interviews, outreach, case investigation, and other recognized investigatory measures.

(i) RESEARCH AND DEVELOPMENT – This section shall not be construed to prohibit public health or scientific research associated with the public health emergency by the COVID-19 public health authority, a nonprofit, or an institute of higher education; or R&D, manufacture, or distribution of a drug, biological product, or vaccine that relates to COVID-19.

(j) LEGAL REQUIREMENTS – Nothing shall be construed to prohibit a good faith response to or compliance with otherwise valid subpoenas, court orders, or other legal process, or to prohibit storage or providing information as otherwise required by law.

(k) APPLICATION TO HIPAA COVERED ENTITIES – This Act does not apply to a "covered entity" or a person acting as a "business associate" under HIPAA (to the extent that such entities or associates are acting in such capacity) or a health care provider. The HHS Secretary shall promulgate guidance on the applicability of requirements similar to those in this section to "covered entities" and "business associates" to reduce duplication.

Sec. 4 – Protecting the Right to Vote

- A government entity may not, and a covered organization may not knowingly facilitate, on the basis of emergency health data, medical condition, or participation or non-participation in a program to collect emergency health data:
  - deny, restrict, or interfere with the right to vote;
  - attempt to deny, restrict, or interfere with the right to vote in an election; or

  - retaliate against an individual for voting.
- An individual may bring a civil action to obtain appropriate relief against a government entity in a federal district court for a violation of this subsection.

Section 5 - Reports on Civil Rights Impacts

The HHS Secretary, in consultation with the U.S. Commission on Civil Rights and the FTC, shall submit to Congress a report that examines the civil rights impact of the collection, use, and disclosure of health information in response to the public health emergency related to the coronavirus. The first report shall be issued not sooner than 9 months, and not later than 12 months, after enactment. Reports shall be issued annually thereafter until 1 year after the last declaration of a public health emergency related to the coronavirus (COVID-19).

Section 6 – Enforcement

(a) FTC –

- The FTC is empowered to treat violations of the Act as an unfair or deceptive act or practice, allowing the FTC to directly assess fines or related penalties for violations.
- The FTC has APA rulemaking authorities to implement this Act and will promulgate regulations in consultation with HHS.

(b) ENFORCEMENT BY STATES –

- A State AG can bring actions, on behalf of a resident.
- The AG must notify the FTC in writing before filing a case.
- The FTC may intervene in a case brought by a state AG.

(c) PRIVATE RIGHT OF ACTION – Any individual alleging a violation of this Act may bring a civil action in any state or federal court.

- The court may award:
  - $100 – $1,000 per violation for negligent violations;
  - $500 - $5,000 per violation for reckless, willful, or intentional violation;
  - attorney's fees; and
  - any other relief, including equitable or declaratory relief, that the court deems appropriate.
- A violation constitutes a concrete and particularized injury in fact to that individual.
- No pre-dispute arbitration agreement or pre-dispute joint-action waiver shall be valid

Section 7 – Non-Preemption

This legislation shall not preempt or supersede any Federal or State law or regulation, or limit the authority of the Commission or the Secretary under any other provision of law.

Section 8 – Effective Date

(a) The Act should apply no later than 30 days after the enactment.

(b) Any person may take actions to come into compliance with this Act before the effective date. The FTC may begin rulemaking before the effective date.