



Comparison Between Bi-Cameral Democratic COVID-19 Privacy Bill & Senate Republican Bill

| Provisions / Definitions | Democrat | Republican |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bill Name | <u>HR 6866, Public Health Emergency Privacy Act</u> | <u>COVID-19 Consumer 4 Data Protection Act of 2020 Summary</u> |
| Sponsors | Rep. Eshoo (D-CA) Rep. Jan Schakowsky (D-IL) Rep. Suzan DelBene (WA-01) Senator Blumenthal (D-CT) Senator Warner (D-VA) | Senators Wicker (R-MS) (lead) Senator Thune (R-SD) Senator Moran (R-KS) Senator Blackburn (R-TN) Senator Fisher (R-NE) |
| Who must comply? | <p>“Covered Organizations” = Any person (including a government entity)</p> <ul style="list-style-type: none"> • that collects, uses, or discloses emergency health data electronically or through communication by wire or radio.; or • develops or operates a website, web application, mobile application, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the public health emergency (notwithstanding the definition of service provider). | <p>“Covered Entity” = Any entity or person that is</p> <ul style="list-style-type: none"> • subject to the <u>Federal Trade Commission Act</u>; or • a common carrier or nonprofit organization described in section 4(a)(4); • collects, processes, or transfers such covered data, or determines the means and purposes for the collection, processing, or transfer of covered data; and • is not a service provider with respect to such data. |



| | | |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Whose excluded from compliance? | Does NOT include— <ul style="list-style-type: none"> • 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; • public health authority. | <ul style="list-style-type: none"> • As noted above compliance is limited to those who must comply with FTC Act which appears to be very broad.^{1,2} |
| HIPAA carve-out? | Yes – bill reads: <ul style="list-style-type: none"> • IN GENERAL.— This Act does not apply to persons “covered entities” subject to the HIPAA Privacy Rule regulations or “business associates” (to the extent that such “business associates” are acting in such capacity), as such terms are defined in the HIPAA regulations, or any health care provider. | No. HIPAA covered entities and business associates are not explicitly carved out, however, protected health information (PHI) under HIPAA is carved out. |

¹ Section 45(a)(2) of the FTC Act, says, “(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C. 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C. 227(b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.”

² According to the FTC, “The Federal Trade Commission Act is the primary statute of the Commission. Under this Act, as amended, the Commission is empowered, among other things, to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress and the public. A number of other statutes listed here are enforced under the FTC Act.”



| | | |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • GUIDANCE FOR CONSISTENCY.— Not later than 30 days after the enactment of this Act, the Secretary shall promulgate guidance on the applicability of requirements of similar to those in this section to persons subject to the HIPAA Privacy Rule regulations or operating as a business associate for a person subject to the HIPAA Privacy Rule Regulations. In promulgating such guidance, the Secretary shall reduce duplication of requirements and may exclude a requirement of this section if such requirement is already a requirement of the HIPAA Privacy Rule regulations. | |
| What data is covered? | Emergency health data which includes but is not limited to genetic, biometrics, data derived from testing, public health surveillance, demographics, geolocation, collected from a personal device. | Precise geolocation data, proximity data, a persistent identifier, and personal health information. |
| What data is excluded? | Silent. | <ul style="list-style-type: none"> • Aggregated data. • Business contact information. • De-identified data. • Employee screening data. • Publicly available information. |
| Privacy / security requirements | Contains a provision requiring reasonable data security policies, practices, and procedures to protect the security and confidentiality of emergency health data. | <p>Requires posting a clear and conspicuous privacy policy within 14 days of the Act's enactment that provides information about data transfers, data retention practices, and data security practices.</p> <p>Also requires covered entities establish, implement, and maintain reasonable administrative, technical,</p> |



| | | |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | and physical data security policies and practices to protect against risks to data. |
| Notice / Consent | “Affirmative express consent” that clearly and conspicuously communicates the individual’s authorization of an act or practice required. Can’t impair user choice to obtain consent and can’t be inferred from non-action. | Prior notice and affirmative express consent for the collection, processing, or transfer of covered data to track COVID-19, monitor social distancing compliance, or for COVID-19 contact tracing purposes |
| Opt Out Rights: | Silent | Giving individuals the right to opt out of such processing |
| Accountability | A covered organization that collects, uses, or discloses emergency health data of at least 100,000 individuals must report aggregate data at least once every 90 on number of individuals whose emergency health data the covered organization collected, used, or disclosed. | During the public health emergency, providing a bi-monthly public report identifying the aggregate number of individuals from whom the covered entity has collected, processed, or transferred covered data for COVID-19 purposes with additional detail about how and why that information was used |
| FTC Enforcement | Federal Trade Commission (FTC) will enforce this bill. Bill also instructs FTC to collaborate with HHS on enforcement. | The FTC has enforcement authority under the bill and would also be required to release data minimization guidelines in relation to COVID-19 processing |
| Data destruction | Covered organization may not use or keep emergency health data the later of— <ul style="list-style-type: none"> • 30 days after the termination of PHE (state or federal); • 30 days after collection. | Covered entity must delete or de-identify all covered data when it is no longer being used for COVID and it’s no longer necessary to comply with legal obligations. |
| For what duration does rights in bill apply? | During any Public Health Emergency including COVID-19 | Limited to during the COVID-19 Public Health Emergency |
| Private right of action | Yes. Allows a court to award— <ul style="list-style-type: none"> • an amount not less than \$100 and not greater than \$1,000 per violation against any person | Silent. |



| | | |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>who negligently violates a provision of this Act;</p> <ul style="list-style-type: none"> • an amount not less than \$500 and not greater than \$5,000 against any person who recklessly, willfully, or intentionally violates a provision of this Act; • reasonable attorney’s fees and litigation costs; and • any other relief, including equitable or declaratory relief, that the court determines appropriate. | |
| State enforcement / preemption | <p>State attorney generals can bring a civil action on behalf of the residents of the State to obtain appropriate relief if they feel they are adversely affected.</p> | <ul style="list-style-type: none"> • No state preemption permitted. • State attorney generals can bring a civil action on behalf of the residents of the State to obtain appropriate relief if they feel they are adversely affected. |
| Effective date | 30 days following enactment. | Silent. |