



GENERAL COMMITTEE MEETING

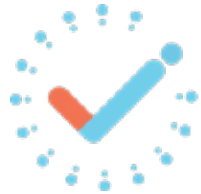
Thursday, May 21, 2020
3:00 PM to 4:00 PM

Dial-In

888-432-1688; Room: 6597; User: 6328

1. Welcome and Introductions
2. Guest speaker
Paul Uhrig, The Commons Project Attachment 1
3. Legislative update
 - a. COVID-19 Consumer Data Protection Act Attachment 2
 - b. Modernizing Health Privacy Act Attachment 3
 - c. Wicker-Blumenthal side-by-side Attachment 4
4. Regulatory update
 - a. FTC comments
<https://www.ftc.gov/news-events/press-releases/2020/05/ftc-seeks-comment-part-review-health-breach-notification-rule>
 - b. CISA cybersecurity warning
<https://www.cisa.gov/news/2020/05/05/cyber-warning-issued-key-healthcare-organizations-uk-and-usa>
 - c. FDA letter Attachment 5
5. Monthly privacy round up Attachment 6

Next Meeting: June 18, 2020 3:00-4:00pm



COVIDcheck

A **CommonHealth** Service

COVIDcheck connects people and communities around the world to help them better understand their COVID status and take the right steps to overcome the pandemic



The Commons Project

Independent Nonprofit Public Trust



The Commons Project

Independent Nonprofit Public Trust

The Commons Project is a 501c3 non-profit public trust, established to build digital services that **put people first**. The Commons Project fills the void between tech companies, government agencies, and traditional non-profits to build and operate the digital services that constitute **public infrastructure** for the digital era.

The Commons Project was established with support from:



Our Principles:

- We serve peoples' interests above all
- People should control their private information
- Our services are not influenced by the interests of any third party
- We operate transparently with partners and people

How can I protect myself, my family and my community?

Do I have COVID-19?

Am I at risk?

What should I do?

Should I get tested?

How can I get more information?

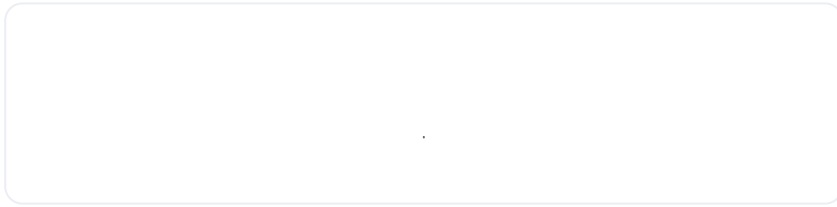
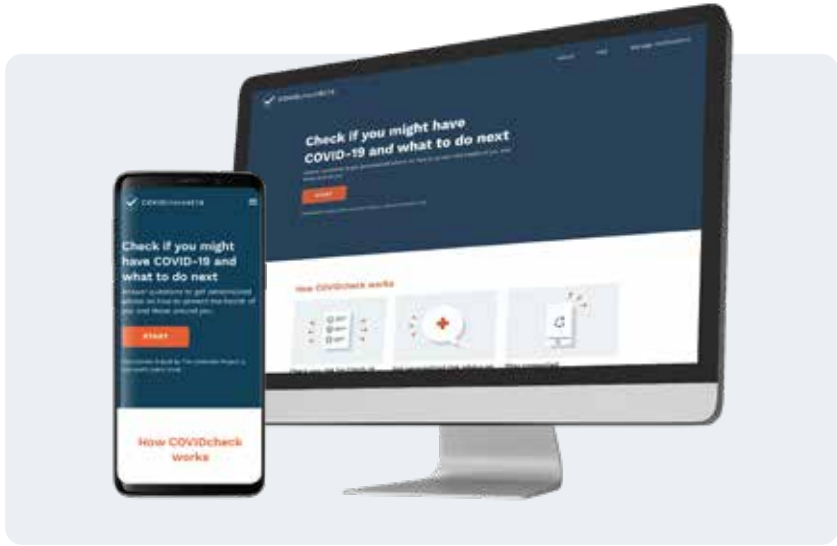
Where can I get help if I am sick?

Can I go back to work?

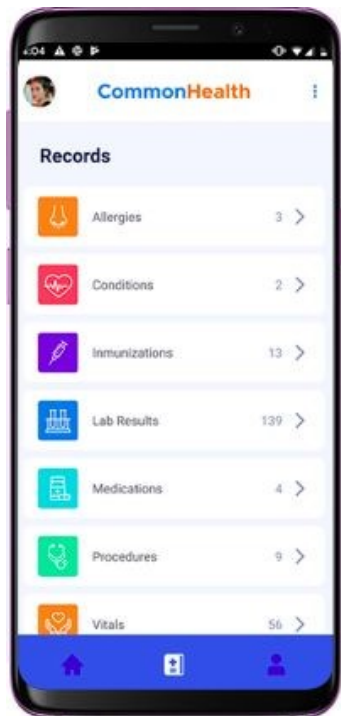
How can I know my immunity status?

How can I share my immunity status securely?

How can I help my community overcome COVID-19?



CommonHealth



CommonHealth is a free public service that lets people collect and store their personal health data and share it securely with the health partners they **trust**

Data is only shared with clear, informed **consent**



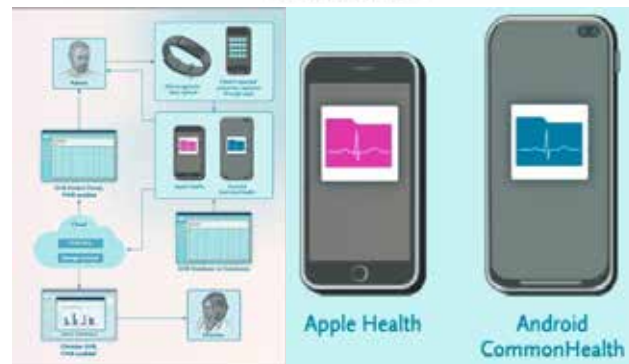
The NEW ENGLAND
JOURNAL of MEDICINE

REVIEW ARTICLE

FRONTIERS IN MEDICINE

Mobile Devices and Health

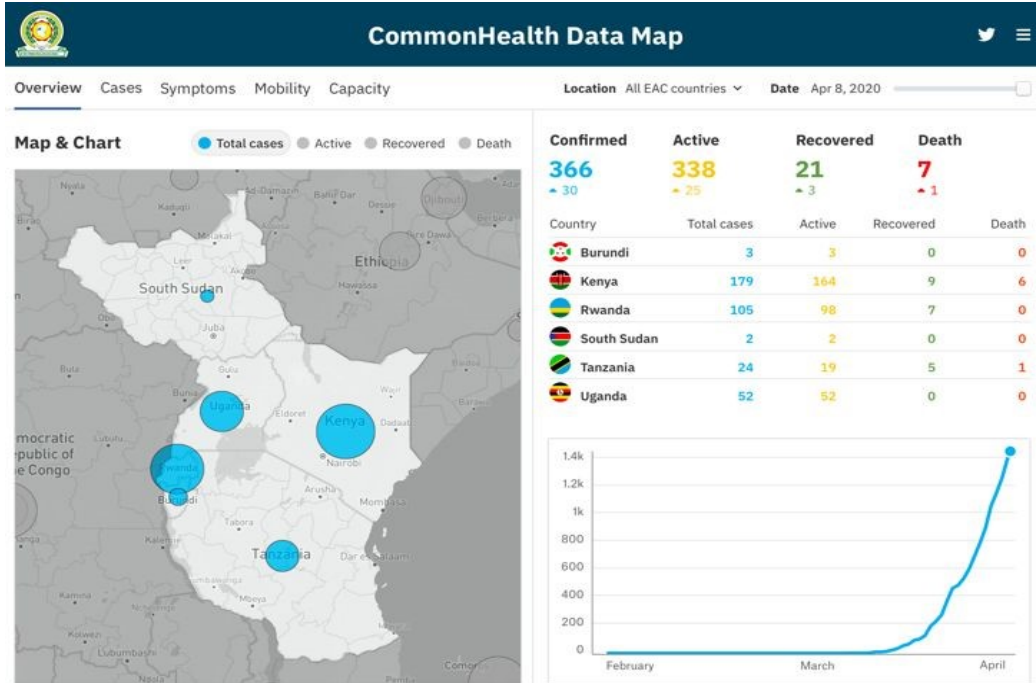
Ida Sim, M.D., Ph.D.



The CommonHealth model was recently featured in the [New England Journal of Medicine](#)

Data Map

A mapping and analytics engine to inform public health and response



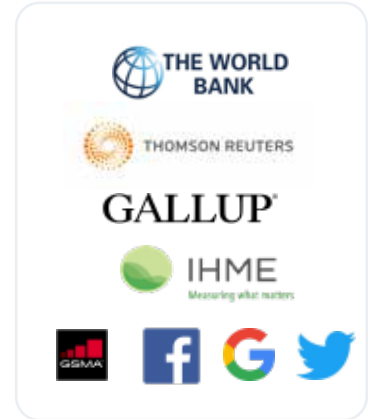
De-identified symptom and other data generated by COVIDcheck users is mapped in real-time to inform public health authorities and COVID response efforts

COVIDcheck aggregate data can be combined with other data sources to give a much richer picture of the pandemic

DATA LAYERS:

- Case Counts
- Capacity
- Mobility
- COVIDcheck Data
 - Reported symptoms
 - Self-diagnostic data
 - Ad-hoc surveys, e.g. Handwashing
 - Social distancing
 - Food availability
 - Community reports

ADDITIONAL DATA SOURCES:



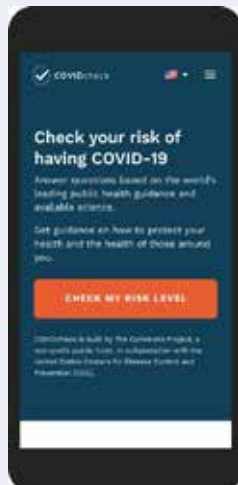


Integrated Model



The Commons Project

Independent Nonprofit Public Trust



CommonHealth DATA TRUST



A framework and repository for people and organizations to share data securely with consent for public health and research purposes.

ADDITIONAL DATA SOURCES



CommonHealth DATA MAP



A mapping and analytics engine to inform public health and response.

for People and the Public Sector

Public Health and Clinical Advisory Board

The algorithms for the COVIDcheck self diagnostic and guidance are developed and maintained under the supervision of the COVIDcheck Public Health and Clinical Advisory Board, which includes physician epidemiologists with extensive global experience in infectious disease.

Brad Perkins, MD, Chair

Chief Medical Officer, The Commons Project. Former Chief Strategy Officer, US Centers for Disease Control and Prevention

Robert Black, MD

Professor and Director of the Institute for International Programs, John Hopkins Bloomberg School of Public Health

Ahmed Ogwell, MD

Deputy Director, Africa Centres for Disease Control and Prevention (CDC Africa)

Michael Osterholm, PhD

Regents Professor, Director, Center for Infectious Disease Research and Policy (CIDRAP)

Marjorie Pollack, MD

Medical Epidemiologist, Deputy Editor, ProMED

David Fleming, MD

Vice President of Public Health, PATH. Former Director of Public Health, Seattle & King County

Ernesto Gozzer, MD

Professor, Cayetano University of Peru. Former Director, National Institute of Health, Peru

Robert Wah, MD

Co-Chair, Health Information Technology Advisory Committee (HITAC), US Department of Health and Human Services. Former President, American Medical Association

Pamela Johnson, PhD

Co-founder, former Chief Health Officer, Voxiva; Global Coordinator for Child Survival, USAID

Andrew Watson, MD

Surgeon & Vice President, UPMC. Former President, American Telemedicine Association

Ivor Braden Horn, MD

Former Chief Medical Officer, Accolade. Former Medical Director -
Center for Diversity & Health Equity, Seattle Children's

TEAM

Executive director of COVIDCheck and was President of the American Medical Association, Global CMO



at CSC, and Associate CIO of the Military Health System.

[Brad Perkins, MD](#) is Chief Medical Officer of The Commons Project overseeing public health and clinical development. He is the former Chief Strategy Officer at CDC and Founding Chief Medical Officer of Human Longevity.

[Ivor Braden Horn, MD](#) was Chief Medical Officer at Accolade and Medical Director, Center for Diversity & Health Equity at Seattle Children's.

[Andrew Watson, MD](#) is a surgeon and VP at UPMC and past president of the American Telemedicine Association.

[Alan Warren, PhD](#) was VP of Engineering at Google and CTO of Oscar Insurance.

[JP Pollak, PhD](#) is Chief Product Officer of The Commons Project overseeing data and privacy. He is a Senior Researcher in Residence at Cornell Tech and Assistant Professor at Weill Cornell Medicine.

[Karen Watson](#) was SVP, Nielsen Government and Public Sector.

[Angela Calman](#) is SVP Communications & Mktg at The Commons Project. She is the former CCO of The Cleveland Clinic and has led global communications for major health and consumer brands.

[Cyrus Kazi](#) is SVP business operations of The Commons Project and was CEO of Quantibly, Founder/CEO of Quantibly, and Managing Director at Lexington Advisory Group.

[Paul Meyer](#) is CEO of The Commons Project. He was founder of Text4baby, co-founder & CEO of Voxiva and Wellpass, co-founder of IPKO Telecom in Kosovo.

[Gabrielle Fitzgerald](#) was Director, Global Program Advocacy at the Gates Foundation and Director of the Paul G. Allen Ebola Program.

[Jean Philbert Nsengimana](#) was Rwanda's Minister for Information & Communications Technology.

[Lesley Edwards](#) was Deputy Director, Life Sciences Partnerships at the Gates Foundation and VP of Partnerships at CommonImpact.

[Pamela Johnson, PhD](#) was Chief Health Officer of Voxiva, Deputy Director of the White House Reinventing Government Initiative and USAID Coordinator for Child Survival.

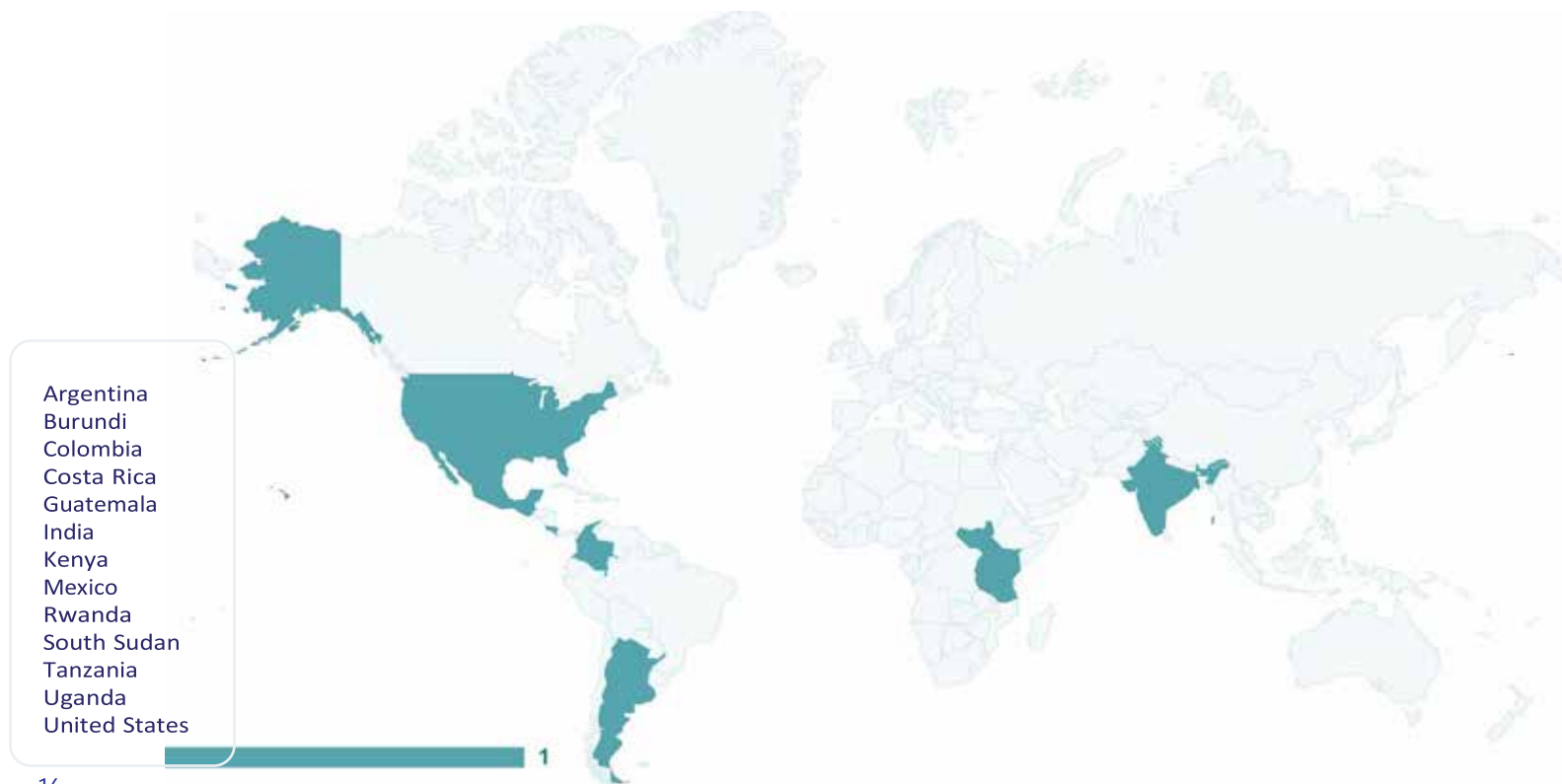
[Frank D'Souza](#) is Vice Chairman and was co-founder and CEO of Cognizant.

[John Boomgard](#) was Senior Product Manager for Amazon Prime.

[Kathryn Tucker](#) is Chief Innovation Officer at The Commons Project, overseeing creative and design. She was CEO of RedRover and is an award winning film producer.

[Thomas Crampton](#) was Global Chair, Digital at Edelman, Global Managing Director, Digital and Social at Ogilvy and foreign correspondent at The New York Times.

Deployments Underway



THANK YOU.

420 Fifth Avenue, 19th Floor
New York, NY 10018
info@thecommonproject.org

 The Commons Project

116TH CONGRESS

2D SESSION

S.

||

To protect the privacy of consumers’ personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis.

IN THE SENATE OF THE UNITED STATES

|||||||

Mr. WICKER (for himself, Mr. THUNE, Mr. MORAN, Mrs. BLACKBURN, and Mrs. FISCHER) introduced the following bill; which was read twice and referred to the Committee on |||||||

A BILL

To protect the privacy of consumers’ personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis.

*1 Be it enacted by the Senate and House of Representa2 tives
of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “COVID–19
Consumer

5 Data Protection Act of 2020”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1

2

3

8

(1) AGGREGATED DATA.—The term “aggre-

9

gated data” means information that—

5VS BK H5Z

(A) relates to a group or category of individuals;

and

(B) does not identify, and is not linked or

4

reasonably linkable to, any individual.

5

(2) AFFIRMATIVE EXPRESS CONSENT.— 6 (A) IN

GENERAL.—The term “affirmative 7 express

consent” means an affirmative act by

8 an individual that—

9 (i) clearly communicates the individ10 ual’s authorization

of an act or practice;

11 and

12 (ii) is taken after the individual has

13 been presented with a clear and con-

14 spicuous description of such act or prac-

15 tice.

23

24

25

1

2

3

16

(B) NO INFERENCE FROM INACTION.—For

17

purposes of subparagraph (A), the affirmative

18

express consent of an individual cannot be in

ferred from inaction.

20

(3) BUSINESS CONTACT INFORMATION.—The

21

term “business contact information” means informa-

22

tion related to an individual’s business position name

or title, business telephone number, business address,

business email address, and other similar business

information, provided that such information

is collected, processed, or transferred solely for

purposes related to such individual’s professional

activi-

ties.

4

(4) COLLECTION.—The term

“collection”

23

24

25

1

2

3

5

means buying, renting, gathering, accessing, or
oth6 erwise acquiring any covered data of an
individual 7 by any means.

8

(5) COMMISSION.—The term “Commission”

9

means the Federal Trade Commission.

10

(6) COVERED DATA.—

11

(A) IN GENERAL.—The term “covered

12

data” means precise geolocation data,
proximity

13

data, a persistent identifier, and personal
health

14

information.

15

(B) EXCLUSIONS.—Such term does not
in-

16

clude the following:

17

(i) Aggregated data.

18

(ii) Business contact information.

19

(iii) De-identified data.

20

(iv) Employee screening data.

23

24

25

1

2

3

21

(v) Publicly available information.

22

(7) COVERED ENTITY.—The term “covered en-

tity” means, with respect to a set of covered data, any entity or person that—

(A) is—

(i) subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); or

(ii) a common carrier or nonprofit or-

4

ganization described in section 4(a)(4);

5

(B) collects, processes, or transfers such

6

covered data, or determines the means and

pur7 poses for the collection, processing, or

transfer 8 of covered data; and

9 (C) is not a service provider with respect 10 to such data.

11 (8) COVID–19 PUBLIC HEALTH EMERGENCY.— 12 The term

“COVID–19 public health emergency” 13 means the period—

14 (A) beginning on the date of enactment of 15 this Act; and

23

24

25

1

2

3

16

(B) ending on the last day of the public

17

health emergency declared by the Secretary
of

18

Health and Human Services pursuant to
section 319 of the Public Health Service
Act (42

20

U.S.C. 247d) on January 31, 2020, entitled

21

“Determination that a Public Health Emer-

22

gency Exists Nationwide as the Result of the 2019
Novel Coronavirus” (including any renewal of
such declaration pursuant to such section 319).

23

24

25

1

2

3

(9) DE-IDENTIFIED DATA.—The term “de-identified data” means information held by a covered entity that—

4

(A) does not identify and is not reasonably

5

linkable to an individual;

6

(B) does not contain any personal identifiers or other information that could be readily

8

used to re-identify the individual to whom the information pertains;

10 (C) is subject to a public commitment by 11 the covered entity—

12

(i) to refrain from attempting to use

13

such information to identify any individual;

14

and

15

(ii) to adopt technical and organiza-

23

24

1

2

3

16

tional measures to ensure that such information is not linked to any individual; and (D) is not disclosed by the covered entity

19 to any other party unless the disclosure is subject to a contractually or other legally binding

21

requirement that—

22

(i) the recipient of the information shall not use the information to identify any individual; and

(ii) all onward disclosures of the information shall be subject to the requirement described in clause (i).

4

(10) EMPLOYEE SCREENING DATA.—The term

5

“employee screening data” means, with respect to a

6

covered entity, covered data of an individual who is

7

an employee, owner, director, officer, staff member,

23

24

1

2

3

8 trainee, vendor, visitor, intern, volunteer, or con9

tractor of the covered entity, provided that such data

10 is only collected, processed, or transferred by the

11 covered entity for the purpose of determining, for

12 purposes related to the COVID–19 public health

13 emergency, whether the individual is permitted to

14 enter a physical site of operation of the covered enti-

15 ty.

16 (11) DELETE.—The term “delete” means to re17 move

or destroy information such that it is not 18 maintained

in human or machine readable form and

19 cannot be retrieved or utilized in the normal course

20 of business.

21 (12) INDIVIDUAL.—

22 (A) IN GENERAL.—The term “individual”

means a natural person residing in the United

States.

23

24

25

1

2

3

(B) EXCLUSION.—Such term does not include, with respect to a covered entity, an individual acting as a full-time or part-time, paid or

4

unpaid employee, owner, director, officer, staff

5

member, trainee, vendor, visitor, intern, volun6

teer, or contractor of a covered entity permitted

7

to enter a physical site of operation of the cov-

8

ered entity.

9

(13) PERSISTENT IDENTIFIER.—The term

10 “persistent identifier” means a technologically de11

rived identifier that identifies an individual, or is

12

linked or reasonably linkable to an individual over

13

time and across services and platforms, which may

14

include a customer number held in a cookie, a static

15

Internet Protocol (IP) address, a processor or device

16

serial number, or another unique device identifier.

23

24

1

2

3

17 (14) PERSONAL HEALTH INFORMATION.— 18 (A) IN

GENERAL.—The term “personal

19 health information” means
information relating

20 to an individual that—

21 (i) is—

22 (I) genetic information of the in-
dividual; or

(II) information relating to the
diagnosis or treatment of past, present,
or future physical, mental health, or
disability of the individual; and

4 (ii) identifies, or is reasonably linkable 5 to, the individual.

6 (B) EXCLUSIONS.—Such term does not in 7 clude the
following:

8 (i) Information from education
9 records that are subject to the require-

23

24

25

1

2

3

10

ments of section 444 of the General
Education Provisions Act (20 U.S.C.
1232g,

commonly referred to as the “Family Educational Rights
and Privacy Act of 1974”)

or from records described in subsection (a)(4)(B)(iv) of
such section.

16

(ii) Information subject to regulations

17

promulgated pursuant to section 264(c)
of

18

the Health Insurance Portability and
Accountability Act of 1996 (42
U.S.C. 201320d–2 note).

21

(15) PRECISE GEOLOCATION DATA.—The term

“precise geolocation data” means technologically derived
information capable of determining with reasonable
specificity the past or present actual phys-

ical location of an individual at a specific point in time.

23

24

1

2

3

(16) PROCESS.—The term “process” means any operation or set of operations performed on covered data, including analyzing, organizing, structuring, retaining, using, or otherwise handling such

7 data.

8

9

10

(17) PROXIMITY DATA.—The term “proximity data” means technologically derived information that identifies the past or present proximity of one individual to another.

12

(18) PUBLICLY AVAILABLE INFORMATION.—

13 The term “publicly available information” means 14 any information that—

15

16

(A) has been lawfully made available to the general public from Federal, State, or local government records; or

18 (B) is widely available to the general public, including information from—

23

24

25

1

2

3

20 (i) a telephone book or online direc-

21 tory;

22 (ii) video, internet, or audio content;

or

(iii) the news media or a website that is available to the general public on an unrestricted basis (for purposes of this subclause a website is not restricted solely because there is a fee or log-in requirement associated with accessing the website).

4

5 (19) SERVICE PROVIDER.—The term “service
6 provider” means, with respect to a set of
covered

7 data, an entity that processes or transfers such cov8 ered data
for the purpose of performing one or more
9 services or functions on behalf of, and at the direc10 tion of,
a covered entity to which it is not related.

11 (20) TRANSFER.—The term “transfer” means

23

24

1

2

3

12 to disclose, release, share, disseminate, or
otherwise

13 make available covered data by any means.

14 **SEC. 3. PRIVACY OF COVERED DATA.**

15 (a) IN GENERAL.—During the COVID–19 public
16 health emergency, it shall be unlawful for a
covered entity

17 to collect, process, or transfer the covered data of
an indi18 vidual for a purpose described in
subsection (b) unless— 19 (1) the covered entity
provides the individual

20 with prior notice of the purpose for such collection, 21
processing, or transfer;

22 (2) the individual has given affirmative express
consent to such collection, processing, or transfer; and

(3) the covered entity publicly commits not to
collect, process, or transfer such covered data for a
purpose other than the purpose described in sub-

23

24

25

1

2

3

4

section (b) to which the individual consented
un-

5

less—

6

(A) such collection, processing, or transfer

7

is necessary to comply with the provisions of

8 this Act or other applicable laws;

9

(B) such collection, processing, or transfer

10

is necessary to carry out operational or

admin11 istrative tasks in support of a purpose

described

12 in subsection (b) to which the individual has 13 consented; or

14

(C) the individual gives affirmative express

15

consent to such collection, processing, or
trans-

16

fer.

17

(b) COVERED PURPOSES.—The purposes
described in

18

this subsection are the following:

19

(1) Collecting, processing, or transferring the

23

24

1

2

3

20

covered data of an individual to track the spread, 21 signs, or symptoms of COVID-19.

22

(2) Collecting, processing, or transferring the covered data of an individual to measure compliance with social distancing guidelines or other requirements related to COVID-19 that are imposed on in-

23

24

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

dividuals under a Federal, State, or local government order.

(3) Collecting, processing, or transferring the covered data of an individual to conduct contact tracing for COVID-19 cases.

(c) TRANSPARENCY.—

(1) PRIVACY POLICY.—A covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall, not later

than 14 days after the enactment of this Act, publish a privacy policy that—

(A) is disclosed in a clear and conspicuous manner to an individual prior to or at the point of the collection of covered data for such a purpose from the individual;

1

2

3

16 (B) is made available in a clear and con-
17 spicuous manner to the public;

18 (C) includes whether, subject to the affirm19
ative express consent requirement of
subsection

20 (a), the covered entity transfers covered data
21 for such a purpose and the categories of recipi-
22 ents to whom the covered entity transfers cov-
ered data for such purpose;

(D) includes a general description of the
covered entity's data retention practices for
covered data used for a purpose described in
subsection (b) and the purposes for such retention;
and

4 (E) includes a general description of the 5 covered entity's
data security practices.

6 (2) REPORTING.—During the COVID–19 public 7 health
emergency, a covered entity that collects,

23

24

25

1

2

3

8 processes, or transfers covered data for a purpose 9 described
in subsection (b) shall issue a public report

10 not later than 30 days after the enactment of
this

11 Act and not less frequently than once every
60 days

12 thereafter—

13 (A) stating in aggregate terms the number

14 of individuals whose covered data the entity
has

15 collected, processed, or transferred for such a

16 purpose; and

17 (B) describing the categories of covered

18 data collected, processed, or transferred by
the

19 entity, the specific purposes for which each
such

20 category of covered data is collected,
processed,

21 or transferred, and, in the case of transferred

23

24

25

1

2

3

22

covered data, to whom such data was transferred.

(d) RIGHT TO OPT-OUT.—During the COVID–19 public health emergency, each covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall do the following:

(1) The covered entity shall provide an effective mechanism for an individual who has consented pursuant to subsection (a) to the collection, processing, or transfer of the individual’s covered data for such a purpose to revoke such consent.

(2) A covered entity that receives a revocation of consent from an individual described in paragraph (1) shall, as soon as practicable but in no case later

11

than 14 days after receiving such revocation, stop

12

collecting, processing, or transferring the covered

13

data of such individual for a purpose described in

14

subsection (b), or shall de-identify all such data.

23

24

25

1

2

3

15 (e) DATA DELETION.—A covered entity shall delete 16 or de-
identify all covered data collected, processed, or
17 transferred for a purpose described in subsection (b) when 18
it is no longer being used for such purpose and is no 19 longer
necessary to comply with a Federal, State, or local
20 legal obligation, or the establishment, exercise, or defense 21
of a legal claim.

22 (f) DATA ACCURACY.—A covered entity shall take reasonable
measures to ensure the accuracy of covered data collected,
processed, or transferred for a purpose described in
subsection (b) and shall provide an effective

23

24

25

1

2

3

mechanism for an individual to report inaccuracies in covered data.

(g) DATA MINIMIZATION.—

4 (1) IN GENERAL.—During the COVID–19 pub-

5 lic health emergency, a covered entity that collects,

6 processes, or transfers covered data for a purpose

7 described in subsection (b) shall not collect, process,

8 or transfer covered data beyond what is reasonably 9

necessary, proportionate, and limited to carry out 10

such purpose.

11 (2) GUIDELINES.—Not later than 30 days after 12 the date of enactment of this Act, the Commission

13 shall issue guidelines recommending best practices

14 for covered entities to minimize the collection, proc15

essing, and transfer of covered data in accordance 16

with this subsection.

23

24

1

2

3

17 (h) PROTECTION OF COVERED DATA.—During the
18 COVID–19 public health emergency, a covered entity that 19
collects, processes, or transfers covered data for a purpose
20 described in subsection (b) shall establish, implement, and
21 maintain reasonable administrative, technical, and phys-
22 ical data security policies and practices to protect against
risks to the confidentiality, security, and integrity of such
data.

(i) EXCEPTION.—Notwithstanding subsection (a), a
covered entity may collect, process, or transfer the covered
data of an individual or group of individuals for a purpose
4 described in subsection (b) during the COVID–19 public
5 health emergency without obtaining the affirmative ex-
6 press consent of the individual if such collection, proc7
essing, or transfer is necessary to allow the covered entity
8 to comply with a Federal, State, or local legal obligation.

9 **SEC. 4. ENFORCEMENT.**

23

24

25

1

2

3

10 (a) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

12

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—

13 TICES.—A violation of this Act shall be treated as 14 a
violation of a regulation under section 18(a)(1)(B) 15 of the
Federal Trade Commission Act (15 U.S.C.

16 57a(a)(1)(B)) regarding unfair or deceptive acts or 17
practices.

18

(2) POWERS OF COMMISSION.—Except as pro-

19

vided in paragraph (4), the Commission shall en20
force this Act in the same manner, by the same

21

means, and with the same jurisdiction, powers, and

22

duties as though all applicable terms and provisions of
the Federal Trade Commission Act (15 U.S.C. 41 et
seq.) were incorporated into and made a part of this Act.

Any person who violates such section shall

be subject to the penalties and entitled to the privileges
and immunities provided in the Federal Trade

Commission Act. Except as provided in subsection

23

24

1

2

3

4 (c), enforcement by the Commission shall be the exclusive
means of enforcing compliance with this Act.

6 (3) COOPERATION WITH OTHER AGENCIES.—

7 Whenever the Commission obtains information that

8 any covered entity may have processed or transferred
covered data in violation of Federal anti-discrimination laws,
the Commission shall transmit the

11 information to the appropriate Federal or State

12 agency with authority to initiate proceedings related
to such violation.

14 (4) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—

15 Notwithstanding section 4, 5(a)(2), or

16 6 of the Federal Trade Commission Act (15 U.S.C. 17

44, 45(a)(2), 46) or any jurisdictional limitation of 18

the Commission, the Commission shall also enforce

19 this Act in the same manner provided in
paragraphs

23

24

25

1

2

3

20 (1) and (2) of this subsection with respect
to—

21 (A) common carriers subject to the Com-

22 munications Act of 1934 (47 U.S.C. 151 et
seq.) and all Acts amendatory thereof and
supplementary thereto; and

(B) organizations not organized to carry on
business for their own profit or that of their
members.

4 (b) EFFECT ON OTHER LAWS.—

5 (1) IN GENERAL.—Nothing in this Act shall be 6 construed in
any way to limit the authority of the 7 Commission under any
other provision of law.

8 (2) NONAPPLICATION OF FCC LAWS AND REGU⁹ LATIONS TO

COVERED ENTITIES.—Notwithstanding

10 any other provision of law, neither any provision of

11 the Communications Act of 1934 (47 U.S.C. 151 et.

23

24

1
2
3
12 seq.) and all Acts amendatory thereof and supple13
mentary thereto nor any regulation promulgated by
14 the Federal Communications Commission under
15 such Acts shall apply to any covered entity with re16
spect to the collection, processing, or transferring of
17 covered data for a purpose described in section 3(b),
18 except to the extent that such provision or regula19 tion
pertains solely to “911” lines or any other
20 emergency line of a hospital, medical provider or
21 service office, health care facility, poison control cen-
22 ter, fire protection agency, or law enforcement agen-
cy.

(3) STATE PREEMPTION.—No State or political
subdivision of a State may adopt, maintain, enforce,

23
24
25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

or continue in effect any law, regulation, rule, requirement, or standard to the extent that such law, regulation, rule, requirement, or standard is related

to the collection, processing, or transfer of covered data for a purpose described in section 3(b).

(c) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—In any case in which the attorney general of a State has reason to believe that

an interest of the residents of that State has been

or is adversely affected by the engagement of any

covered entity in an act or practice that violates this

Act, the attorney general of the State, as *parens*

patriae, may bring a civil action on behalf of the

residents of the State in an appropriate district court of the United States to—

1

2

3

17 (A) enjoin that act or practice;

18 (B) enforce compliance with this Act or the

19 regulation;

20 (C) obtain damages, civil penalties, restitu21

tion, or other compensation on behalf of the

22 residents of the State; or

(D) obtain such other relief as the court may consider to be appropriate.

(2) RIGHTS OF THE COMMISSION.—

(A) IN GENERAL.—Except where not feasible, the attorney general of a State shall notify the Commission in writing prior to initi4 ating a civil action under paragraph (1).

Such

5 notice shall include a copy of the complaint to

6 be filed to initiate such action. Upon receiving

7 such notice, the Commission may intervene in 8

such action and, upon intervening—

9 (i) be heard on all matters arising in

23

24

25

1

2

3

10 such action; and

11 (ii) file petitions for appeal of a deci12
12 sion in such action.

13 (B) NOTIFICATION TIMELINE.—Where it is
14 not feasible for the attorney general of a State
15 to provide the notification required by subpara16
16 graph (A) before initiating a civil action under
17 paragraph (1), the attorney general shall notify
18 the Commission immediately after initiating the
19 civil action.

20 (3) ACTIONS BY COMMISSION.—In any case in
21 which a civil action is instituted by the
22 Commission
23 for violation of this Act, no attorney general of a
24 State may, during the pendency of such action,
25 institute a civil action against any defendant
named in the complaint in the action instituted by
the Com-

23

24

25

1

2

3

mission for a violation of this Act that is alleged in such complaint.

(4) INVESTIGATORY POWERS.—Nothing in this Act shall be construed to prevent the attorney general of a State or another authorized official of a

State from exercising the powers conferred on the attorney general or the State official by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

10

11

12

13

14

15

16

23

24

25

(5) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL OR AUTHORIZED STATE GOVERNMENTAL AUTHORITIES.—Whenever a civil action under paragraph (1) is pending and another civil action or actions are commenced pursuant to such paragraph in a different

1

2

3

18 Federal district court or courts that involve 1 or
19 more common questions of fact, such action or ac20
tions shall be transferred for the purposes of consoli21
dated pretrial proceedings and trial to the United
22 States District Court for the District of Columbia; provided
however, that no such action shall be transferred if
pretrial proceedings in that action have been concluded
before a subsequent action is filed by

23

24

25

1

2

a State attorney general or authorized State governmental authority.

116TH CONGRESS

2D SESSION

S.

||

To protect the privacy of health information during a national health emergency.

IN THE SENATE OF THE UNITED STATES

|||||||

Mr. BLUMENTHAL (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on
|||||||

A BILL

To protect the privacy of health information during a national health emergency.

*1 Be it enacted by the Senate and House of Representa2 tives
of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the ‘‘Public Health Emer-
5 gency Privacy Act’’.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1

2

3

8

(1) AFFIRMATIVE EXPRESS CONSENT.—The

9

term “affirmative express consent” means an affirm-

10

ative act by an individual that—

(A) clearly and conspicuously commu-

nicates the individual’s authorization of an act or
practice;

4 (B) is made in the absence of any mecha5 nism in the user
interface that has the purpose

6

or substantial effect of obscuring, subverting,
or

7

impairing decision making or choice to
obtain

8

consent; and

9

(C) cannot be inferred from inaction.

10

(2) COLLECT.—The term “collect”, with
re11 spect to emergency health data, means
obtaining in 12 any manner by a covered
organization.

13

(3) COMMISSION.—The term “Commission”

22

23

24

25

1

2

14 means the Federal Trade Commission.

15 (4) COVERED ORGANIZATION.— 16 (A) IN

GENERAL.—The term “covered or-

17 ganization” means any person
(including a gov-

18 ernment entity)—

19 (i) that collects, uses, or discloses

20 emergency health data electronically or

21 through communication by wire or
radio;

or

(ii) 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

3 tracing, or mitigation, or otherwise re4 sponding to the
COVID–19 public health

5 emergency.

6 (B) EXCLUSIONS.—The term “covered or-

7 ganization” does not include— 8 (i) a

health care provider;

1

2

3

9 (ii) a person engaged in a de minimis
10 collection or processing of emergency
11 health data;

12 (iii) a service provider;

13 (iv) a person acting in their individual
14 or household capacity; or

15 (v) a public health authority.

16 (5) DEMOGRAPHIC DATA.—The term
“demo-

17 graphic data” means information
relating to the actual or perceived
race, color, ethnicity, national origin,
religion, sex, gender, gender identity,
sexual orientation, age, Tribal
affiliation, disability, domicile,

21 employment status, familial status, immigration status, or
22 veteran status of an individual or group of

23 individuals.

22

23

24

25

1

2

(6) DEVICE.—The term “device” means any electronic equipment that is primarily designed for or marketed to consumers.

4

5

6

7

(7) DISCLOSURE.—The term “disclosure”, with respect to emergency health data, means the releasing, transferring, selling, providing access to, licensing, or divulging in any manner by a covered organization to a third party.

9

10

11

12

13

14

15

16

17

18

(8) EMERGENCY HEALTH DATA.—The term “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—

(A) information that reveals the past,

present, or future physical or behavioral health

1

2

3

19

or condition of, or provision of healthcare to,
an individual, including—

21

(i) data derived from the testing or
examination of a body part or bodily
substance, or a request for such testing;

(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 dis-

3

order; and

4

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

6

(B) other data collected in conjunction

7

with other emergency health data or for the

8

purpose of tracking, screening, monitoring,
contact tracing, or mitigation, or otherwise

re-

10

sponding to the COVID-19 public
health emer-

22

23

24

25

1
2
11 gency, including—
12 (i) geolocation data, when such term
13 means data capable of determining the
14 past or present precise physical location
of
15 an individual at a specific point in time,
16 taking account of population densities,
in-
17 cluding cell-site location information,
tri18 angulation data derived from
nearby wire-
19 less or radio frequency networks, and
glob-
20 al positioning system data;
21 (ii) proximity data, when such term
22 means information that identifies or esti-
23 mates the past or present physical prox-
24 imity of one individual or device to an25
other, including information derived
from Bluetooth, audio signatures,
nearby wireless networks, and near-field
communica-

1

2

3

tions;

4 (iii) demographic data;

5 (iv) contact information for identifi-

6 able individuals or a history of the individ7 ual's contacts
over a period of time, such 8 as an address book or call log; and

9 (v) any other data collected from a 10 personal device.

11 (9) GOVERNMENT ENTITY.—The term “govern-
12 ment entity” includes a Federal agency, a State, a
13 local government, and other organizations, as such
14 terms are defined in section 3371 of title 5, United
15 States Code.

16 (10) HEALTH CARE PROVIDER.—The term
17 “health care provider” has the meaning given the 18 term
“eligible health care provider” in title VIII of 19 division B the
CARES Act (Public Law 116–136).

20 (11) HIPAA REGULATIONS.—The term
21 “HIPAA regulations” means parts 160 and 164 of
title 45, Code of Federal Regulations.

22

23

24

25

1

2

(12) PUBLIC HEALTH AUTHORITY.—The term “public health authority” means an entity that is authorized by law to collect or receive 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, and a person, such as a designated agency or associate, acting under a grant of authority from, or under a contract with, such public entity, including the employees or agents of such entity or its contractors or persons or entities to whom it has granted authority.

12 (13) COVID–19 PUBLIC HEALTH EMER-
13 GENCY.—The term “COVID–19 public health emer14
gency” means the outbreak and public health re15 sponse
pertaining to Coronavirus Disease 2019
16 (COVID–19), associated with the emergency de17 clared by
the Secretary on January 31, 2020, under 18 section 319 of the
Public Health Service Act (42 19 U.S.C. 247d), and any renewals
thereof and any

1

2

3

20 subsequent declarations by the Secretary related to 21 the
coronavirus.

22 (14) SECRETARY.—The term “Secretary”

23 means the Secretary of Health and Human
Services.

24 (15) SERVICE PROVIDER.—

(A) IN GENERAL.—The term “service
provider” means a person that collects, uses, or discloses
emergency health data for the sole 4 purpose of, and only to the
extent that such en5 tity is, conducting business activities on
behalf

6 of, for the benefit of, under instruction of, and

7 under contractual agreement with a covered or-

8 ganization.

9 (B) LIMITATION OF APPLICATION.—Such

10 person shall only be considered a service pro11 vider in the
course of activities described in 12 subparagraph (A).

13 (C) EXCLUSIONS.—The ter “service pro-

22

23

24

25

1

2

14 vider” excludes a person that develops or oper-

15 ates a website, web application, mobile applica16 tion, or smart device application for the purpose

17 of tracking, screening, monitoring, contact trac18 ing, or mitigation, or otherwise responding to 19 the COVID–19 public health emergency.

20 (16) STATE.—The term “State” means each

21 State of the United States, the District of Columbia, each commonwealth, territory, or possession of the

United States, and each federally recognized Indian Tribe.

(17) THIRD PARTY.—

(A) IN GENERAL.—The term “third party” means, with respect to a covered organization—

3 (i) another person to whom such cov4 ered organization disclosed emergency 5 health data; and

6 (ii) a corporate affiliate or a related

7 party of the covered organization that does

1

2

3

8 not have a direct relationship with an indi9 vidual with whom the emergency health 10 data is linked or is reasonably linkable.

11

(B) EXCLUSION.—The term “third party”

12

excludes, with respect to a covered organiza-

13

tion—

14

(i) a service provider of such covered

15

organization; or

16

(ii) a public health authority.

17

(18) USE.—The term “use”, with respect to

18

emergency health data, means the

processing, em19 ployment,

application, utilization, examination, or

20 analysis of such data by a covered organization that 21

maintains such data.

22

SEC. 3. PROTECTING THE PRIVACY AND SECURITY OF

22

23

24

25

1

2

23

EMERGENCY HEALTH DATA.

24

(a) **RIGHT TO PRIVACY.**—A covered organization that

25

collects emergency health data shall—

(1) only collect, use, or disclose such data that is necessary, proportionate, and limited for a good faith public health purpose, including a service or 4 feature to support such a purpose;

5

(2) take reasonable measures, where possible, to

6

ensure the accuracy of emergency health data and

7

provide an effective mechanism for an individual to

8

correct inaccurate information;

9

(3) adopt reasonable safeguards to prevent un10 lawful discrimination on the basis of emergency

11

health data; and

12

(4) only disclose such data to a government en-

13

tity when the disclosure—

14

(A) is to a public health authority; and

15

(B) is made in solely for good faith public

16

health purposes and in direct response to
exi17 gent circumstances.

1

2

3

18 (b) RIGHT TO SECURITY.—A covered organization or
19 service provider that collects, uses, or discloses
emergency 20 health data shall establish and implement
reasonable data

21 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—

(1) commercial advertising, recommendation for
e-commerce, or the training of machine-learning al-

3 gorithms related to, or subsequently for use in,
com-

4 mercial advertising and e-commerce;

5 (2) soliciting, offering, selling, leasing, licensing,

6 renting, advertising, marketing, or otherwise com-

22

23

24

25

1

2

7

mercially contracting for employment, finance,
cred8 it, insurance, housing, or education
opportunities in

9 a manner that discriminates or otherwise makes op10
portunities unavailable on the basis of emergency 11 health data;
and

12

(3) segregating, discriminating in, or otherwise

13

making unavailable the goods, services, facilities,

14

privileges, advantages, or accommodations of any

15

place of public accommodation (as such term is de-

16

fined in section 301 of the Americans With Disabil-

17

ities Act of 1990 (42 U.S.C. 12181)), except as
au18 thorized by a State or Federal Government
entity

19

for a public health purpose notwithstanding sub-

20

section (g).

21

(d) CONSENT.—

22

(1) IN GENERAL.—It shall be unlawful for a

23

covered organization to collect, use, or disclose emer-

1

2

3

24 agency health data, unless—

(A) the individual to whom the data pertains has given affirmative express consent to such collection, use, or disclosure;

4

(B) such collection, use, or disclosure is

5

necessary and for the sole purpose of—

6

(i) protecting against malicious, de-

7

ceptive, fraudulent, or illegal activity; or

8

(ii) detecting, responding to, or preventing information security incidents

or

10

threats; or

11

(C) the covered organization is compelled

12

to do so by a legal obligation.

13

(2) REVOCATION.—

14

(A) IN GENERAL.—A covered organization

22

23

24

25

1

2

15 shall provide an effective mechanism for an
in16 dividual to revoke consent after it is
given.

17 (B) EFFECT.—After an individual revokes 18 consent, the
covered organization shall cease 19 collecting, using, or
disclosing the individual's

20 emergency health data as soon as practicable,

21 but in no case later than 15 days after the re-
ceipt of the individual's revocation of consent.

(C) DESTRUCTION.—Not later than 30
days after the receipt of an individual's revocation
of consent, a covered organization shall destroy or
render not linkable that individuals emergency
health data under the same proce-

3 dures in subsection (f).

4 (e) NOTICE.—A covered organization that collects,
5 uses, or discloses emergency health data shall
provide to

6 an individual a privacy policy that—

7 (1) is disclosed in a clear and conspicuous man8 ner, in the
language in which the individual typically 9 interacts with
the covered organization, prior to or

1

2

3

10 at the point of the collection of emergency health

11 data;

12 (2) describes how and for what purposes the

13 covered organization collects, uses, and discloses

14 emergency health data, including the categories of

15 recipients to whom it discloses data and the
purpose

16 of disclosure for each category;

17 (3) describes the covered organization's data re18

retention and data security policies and practices for

19 emergency health data; and

20 (4) describes how an individual may exercise

21 the rights under this Act and how to contact the

22 Commission to file a complaint.

23 (f) PUBLIC REPORTING.—

24 (1) IN GENERAL.—A covered organization that

22

23

24

25

1

2

25

collects, uses, or discloses emergency health data of at least 100,000 individuals shall, at least once every 90 days, issue a public report—

4

5

6

7

8

9

10

13

14

15

16

17

18

19

(A) stating in aggregate terms the number of individuals whose emergency health data the

covered organization collected, used, or disclosed to the extent practicable; and

(B) describing the categories of emergency health data collected, used, or disclosed, the purposes for which each such category of emergency health data was collected, used, or

disclosed, and the categories of third parties to whom it was disclosed.

(2) RULES OF CONSTRUCTION.—Nothing in this subsection shall be construed to require a covered organization to—

(A) take an action that would convert data that is not emergency health data into emergency health data;

(B) collect or maintain emergency health

1

2

3

20

data that the covered organization would
other-

21

wise not maintain; or

(C) maintain emergency health data longer
than the covered organization would otherwise
maintain such data.

(g) REQUIRED DATA DESTRUCTION.—

22

23

24

25

1

2

(1) IN GENERAL.—A covered organization may not use or maintain emergency health data of an individual after the later of—

4

(A) the date that is 60 days after the ter-

5

mination of the public health emergency de6

clared by the Secretary on January 31, 2020,

7

pertaining to Coronavirus Disease
2019

8

(COVID–19) under section 319 of Public 9 Health

Service Act (42 U.S.C. 247d) and any

10

renewals thereof;

11

(B) the date that is 60 days after the ter12

mination of a public health emergency

declared

13 by a governor or chief executive of a State per14 taining to

Coronavirus Disease 2019 (COVID– 15 19) in which the

individual resides; or

16

(C) 60 days after collection.

22

23

24

1

2

3

17 (2) REQUIREMENT.—For the requirements

18 under paragraph (1), data shall be destroyed
or rendered not linkable in such a manner
that it is impossible or demonstrably
impracticable to identify any individual
from the data.

(3) RELATION TO CERTAIN REQUIREMENTS.—

The provisions of this subsection shall not supersede
any requirements or authorizations under—

(A) the Privacy Act of 1974 (Public Law
93–79);

(B) the HIPPA regulations; or

4 (C) Federal or State medical records retention and health
privacy laws or regulations, or 6 other applicable Federal or
State laws.

7 (h) EMERGENCY DATA COLLECTED, USED, OR DIS-

22

23

24

25

1

2

3

8 CLOSED BEFORE ENACTMENT.—

9

(1) INITIATING A RULEMAKING.—Not later

10

than 7 days after the date of enactment of this Act,

11

the Commission shall initiate a public rulemaking to

12

promulgate regulations to ensure a covered organiza13

tion that has collected, used, or disclosed emergency

14

health data before the date of enactment of this Act

15

is in compliance with this Act, to the degree prac16

ticable.

17

(2) COMPLETING A RULEMAKING.—The Com-

18

mission shall complete the rulemaking within 45 19 days after

the date of enactment of this Act.

20

(i) NON-APPLICATION TO MANUAL CONTACT TRAC-

21

ING AND CASE INVESTIGATION.—Nothing in this Act shall

be construed to limit or prohibit a public health authority

from administering programs or activities to identify

22

23

24

25

1

2

3

individuals who have contracted, or may have been exposed to, COVID–19 through interviews, outreach, case investigation, and other recognized investigatory measures by a public health authority or their designated agent by a public health authority or their designated agent intended to monitor and mitigate the transmission of a disease or disorder.

6 (j) RESEARCH AND DEVELOPMENT.—This section

7 shall not be construed to prohibit—

8 (1) public health or scientific research associated with the COVID–19 public health emergency

10 by—

11 (A) a public health authority;

12 (B) a nonprofit organization, as described

13 in section 501(c)(3) of the Internal Revenue
14 Code of 1986; or

15 (C) an institution of higher education, as

22

23

24

25

1

2

3

16 such term is defined in section 101 of the
High17 er Education Act of 1965 (20 U.S.C.
1001); or

18 (2) research, development, manufacture, or dis19 tribution of
a drug, biological product, or vaccine

20 that relates to a disease or disorder that is associ-

21 ated or potentially associated with a public health
emergency.

(k) LEGAL REQUIREMENTS.—Notwithstanding sub-
section (a)(5), nothing in this Act shall be construed to
prohibit a good faith response to, or compliance with,
otherwise valid subpoenas, court orders, or other legal
processes, or to prohibit storage or providing information as
otherwise required by law.

4 (l) APPLICATION TO HIPAA COVERED ENTITIES.— 5 (1) IN
GENERAL.—This Act does not apply to

6 a “covered entity” or a person acting as a “business

22

23

24

25

1

2

3

7 associate’’ under the HIPAA regulations (to the ex8
tent that such entities or associates are acting in 9 such
capacity) or any health care provider.

10 (2) GUIDANCE FOR CONSISTENCY.—Not later

11 than 30 days after the date of enactment of this

12 Act, the Secretary shall promulgate guidance on the

13 applicability of requirements, similar to those in this

14 section to ‘‘covered entities’’ and persons acting as

15 ‘‘business associates’’ under the HIPAA regulations.

16 In promulgating such guidance, the Secretary shall

17 reduce duplication of requirements and may exclude

18 a requirement of this section if such requirement is

19 already a requirement of the HIPAA regulations.

20 **SEC. 4. PROTECTING THE RIGHT TO VOTE.**

21 (a) IN GENERAL.—A government entity may not, and a
covered organization may not knowingly facilitate, on

22

23

24

25

1

2

3

the basis of an individual’s emergency health data, medical condition, or participation or non-participation in a program to collect emergency health data—

(1) deny, restrict, or interfere with the right to vote in a Federal, State, or local election;

4

(2) attempt to deny, restrict, or interfere with

the right to vote in a Federal, State, or local elec-

5

tion; or

6

(3) retaliate against an individual for voting in 7 a Federal, State, or local election.

8 (b) CIVIL ACTION.—In the case of any violation of 9

subsection (a), an individual may bring a civil action to

10 obtain appropriate relief against a government entity in

11 a Federal district court.

12 **SEC. 5. REPORTS ON CIVIL RIGHTS IMPACTS.**

22

23

24

25

1

2

3

13 (a) REPORT REQUIRED.—The Secretary, in consulta14 tion
with the United States Commission on Civil Rights
15 and the Commission, shall prepare and submit to Con16 gress
reports that examines the civil rights impact of the
17 collection, use, and disclosure of health information in re18
sponse to the COVID–19 public health emergency.

19 (b) SCOPE OF REPORT.—Each report required under 20
subsection (a) shall, at a minimum—

21 (1) evaluate the impact of such practices on
civil rights and protections for individuals based on
race, color, ethnicity, national origin, religion, sex,
gender, gender identity, sexual orientation, age,

Tribal affiliation, disability, domicile, employment
status, familial status, immigration status, or veteran
status;

(2) analyze the impact, risks, costs, legal con-
4 siderations, disparate impacts, and other implica-

22

23

24

25

1

2

3

5 tions to civil rights of policies to incentivize or require
the adoption of digital tools or apps used for

7 contact tracing, exposure notification, or health 8 monitoring;

and

9 (3) include recommendations on preventing and

10 addressing undue or disparate impact, segregation,

11 discrimination, or infringements of civil rights in
the

12 collection and use of health information, including

13 during a national health emergency.

14 (c) TIMING.—

15 (1) INITIAL REPORT.—The Secretary shall submit
an initial report under subsection (a) not sooner

17 than 9 months, and not later than 12 months after 18 the date
of enactment of this Act.

19 (2) SUBSEQUENT REPORTS.—The Secretary

20 shall submit reports annually after the initial report

22

23

24

25

1

2

3

21

required under paragraph (1) until 1 year after the termination of any public health emergency pertaining to Coronavirus Disease 2019 (COVID-19) under section 319 of Public Health Service Act (42 U.S.C. 247d).

22

23

24

25

1

2

3

SEC. 6. ENFORCEMENT.**(a) FEDERAL TRADE COMMISSION.—****(1) UNFAIR OR DECEPTIVE ACTS OR PRAC-**

4 TICES.—A violation of this Act or a regulation pro⁵ mulgated
under this Act shall be treated as a viola⁶ tion of a rule defining
an unfair or deceptive act or

7 practice under section 18(a)(1)(B) of the Federal

8 Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) re⁹
garding unfair or deceptive acts or practices.

10 (2) POWERS OF COMMISSION.—The Commis-

11 sion shall enforce this Act and the regulations pro¹² mulgated
under this Act in the same manner, by the

13 same means, and with the same jurisdiction, powers,

14 and duties as though all applicable terms and provi¹⁵
sions of the Federal Trade Commission Act (15

16 U.S.C. 41 et seq.) were incorporated into and made

17 a part of this Act. Any person who violates this Act 18
or a regulation promulgated under this Act shall be

19 subject to the penalties and entitled to the privileges

20 and immunities provided in the Federal Trade Com-

1

2

3

21 mission Act. Provided, however, that, notwith22
standing the requirements of section 16(a) of the 23
Federal Trade Commission Act (15 U.S.C. 56(a)),
24 the Commission shall have the exclusive authority to
25 commence or defend, and supervise the litigation of,
26 any action for a violation of this Act or a regulation
promulgated under this Act and any appeal of such
action in its own name by any of its attorneys
designated by it for such purpose, without first refer-
4 ring the matter to the Attorney General.

5 (3) RULEMAKING AUTHORITY.— 6 (A) IN GENERAL.—

The Commission shall

7 have authority under section 553 of title 5,

8 United States Code, to promulgate any regula9
tions necessary to implement this Act.

10 (B) CONSULTATION.—In promulgating any 11 regulations
under this Act, the Commission 12 shall consult with the
Secretary.

22

23

24

25

1

2

3

13

(4) COMMON CARRIERS AND NONPROFIT ORGA-

14

NIZATIONS.—Notwithstanding section 4, 5(a)(2), or

15

6 of the Federal Trade Commission Act (15 U.S.C. 16

44; 45(a)(2); 46) or any jurisdictional limitation of

17

the Commission, the Commission shall also enforce

18

this Act, in the same manner provided in paragraphs 19

(1) and (2) of this paragraph, with respect to— 20 (A)

common carriers subject to the Acts to

21

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 (7 U.S.C. 181 et seq.),

except as provided in section 406(b) of such Act

(7 U.S.C. 227(b)); and

(B) organizations not organized to carry

4

on business for their own profit or that of their

5

members.

22

23

24

25

1

2

3

6 (b) ENFORCEMENT BY STATES.—

7 (1) IN GENERAL.—In any case in which the attorney general
of a State has reason to believe that an interest of the residents
of the State has been or

10 is threatened or adversely affected by the engagement of
any person subject to this Act in a practice

12 that violates such subsection, the attorney general of

13 the State may, as *parens patriae*, bring a civil action

14 on behalf of the residents of the State in an appropriate
15 district court of the United States to obtain
16 appropriate relief.

17 (2) RIGHTS OF THE FEDERAL TRADE COMMISSION.—

19 (A) NOTICE TO FEDERAL TRADE COMMISSION.—

20 SION.—

21 (i) IN GENERAL.—Except as provided
in clause (iii), the attorney general of a State
shall notify the Commission in writing that
the attorney general intends to bring a civil

22

23

24

25

1

2

3

action under paragraph (1) before initiating the civil action against a person subject to this Act.

4

5

(ii) CONTENTS.—The notification required by clause (i) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

7

8

(iii) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notification required by clause (i)

before initiating a civil action under paragraph (1), the attorney general shall notify

the Commission immediately upon instituting the civil action.

14

(B) INTERVENTION BY THE FEDERAL

TRADE COMMISSION.—The Commission may— (i) intervene in any civil action

22

23

24

25

1

2

3

17

brought by the attorney general of a State

18

under paragraph (1); and

19

(ii) upon intervening— 20 (I) be heard on all

matters aris-

21

ing in the civil action; and

(II) file petitions for appeal of a

decision in the civil action.

(C) INVESTIGATORY POWERS.—Nothing in this

subsection may be construed to prevent the

22

23

24

25

1

2

attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of 6 documentary or other evidence.

7

(3) ACTION BY THE FEDERAL TRADE COMMIS-

8 SION.—If the Commission institutes a civil action 9 with respect to a violation of this Act, the attorney

10

general of a State may not, during the pendency of

11

such action, bring a civil action under paragraph (1)

12

of this subsection against any defendant named in

13

the complaint of the Commission for the violation

14

with respect to which the Commission instituted

15

such action.

16

(4) VENUE; SERVICE OF PROCESS.— 17 (A) VENUE.—

Any action brought under 18 paragraph (1) may be brought in—

19

(i) the district court of the United

22

23

24

1

2

20 States that meets applicable requirements

21 relating to venue under section 1391 of title 28, United States Code; or

(ii) another court of competent jurisdiction.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be

3 served in any district in which the defendant—

4 (i) is an inhabitant; or

5 (ii) may be found.

6 (C) ACTIONS BY OTHER STATE OFFI-

7 CIALS.—

8 (i) IN GENERAL.—In addition to civil 9 actions brought by attorneys general under

10 paragraph (1), any other officer of a State

11 who is authorized by the State to do so 12 may bring a civil action under paragraph

13 (1), subject to the same requirements and

22

23

24

1
2
14 limitations that apply under this sub-
15 section to civil actions brought by attor-
16 neys general.
17 (ii) SAVINGS PROVISION.—Nothing in
18 this subsection may be construed to
prohibit an authorized official of a
State from initiating or continuing
any proceeding in
21 a court of the State for a violation of any
civil or criminal law of the State.

(c) PRIVATE RIGHT OF ACTION.— (1)

ENFORCEMENT BY INDIVIDUALS .—

(A) IN GENERAL.—Any individual alleging a
violation of this Act may bring a civil action
3 in any court of competent jurisdiction, State
or
4 Federal.
5 (B) RELIEF.—In a civil action brought
6 under paragraph (1) in which the plaintiff
pre-
7 vails, the court may award—

1

2

8

(i) an amount not less than \$100 and 9 not greater than \$1,000 per violation

10 against any person who negligently violates 11 a provision of this Act;

12

(ii) an amount not less than \$500 and

13

not greater than \$5,000 per violation

14

against any person who recklessly, will15 fully, or intentionally violates a provision of

16

this Act;

17

(iii) reasonable attorney’s fees and

18

litigation costs; and

19

(iv) any other relief, including equi20 table or declaratory relief, that the court 21 determines appropriate.

22 (C) INJURY IN FACT.—A violation of this 23 Act with respect to the emergency health data

24 of an individual constitutes a concrete and par25 ticularized injury in fact to that individual.

22

23

24

1

2

(2) INVALIDITY OF PRE-DISPUTE ARBITRATION

AGREEMENTS AND PRE-DISPUTE JOINT ACTION 3

WAIVERS.—

4

(A) IN GENERAL.—Notwithstanding any

5

other provision of law, no pre-dispute arbitra-

6

tion agreement or pre-dispute joint action

waiv7 er shall be valid or enforceable with

respect to 8 a dispute arising under this Act.

9

(B) APPLICABILITY.—Any determination

10

as to whether or how this subsection applies to

11

any dispute shall be made by a court, rather

12

than an arbitrator, without regard to whether

13

such agreement purports to delegate such

deter14mination to an arbitrator.

15

(C) DEFINITIONS.—In this subsection:

16

(i) The term “pre-dispute arbitration

17

agreement” means any agreement to

arbi18trate a dispute that has not arisen

at the 19 time of making the agreement.

20

(ii) The term “pre-dispute joint-action

21 waiver” means an agreement, whether
or
22 not part of a pre-dispute arbitration
agree²³ment, that would prohibit, or
waive the
24 right of, one of the parties to the agree-
25 ment to participate in a joint, class, or
collective action in a judicial, arbitral,
administration, or other forum, concerning a dis-
3 pute that has not yet arisen at the time of 4 making the
agreement.

5 (iii) The term “dispute” means any
6 claim related to an alleged violation of
this
7 Act and between an individual and a
cov-
8 ered organization.

9 **SEC. 7. NONPREEMPTION.**

10 Nothing in this Act shall preempt or
supersede, or
11 be interpreted to preempt or supersede,
any Federal or
12 State law or regulation, or limit the
authority of the Com¹³mission or the

1

2

Secretary under any other provision of
law.

14 **SEC. 8. EFFECTIVE DATE.**

15 (a) **IN GENERAL.**—This Act shall apply beginning on 16 the
date that is 30 days after the date of enactment of 17 this
Act.

18 (b) **AUTHORITY TO PROMULGATE REGULATIONS AND**
19 **TAKE CERTAIN OTHER ACTIONS.**—Nothing in
subsection

20 (a) affects—

21 (1) the authority of any person to take an ac-
22 tion expressly required by a provision of this Act
be23 fore the effective date described in such
subsection;

24 or

30

1 (2) the authority of the Commission to promul2 gate regulations
to implement this Act or begin a

3 rulemaking to promulgate such regulations.

Comparison of COVID-19 Contact Tracing Bills

	COVID–19 Consumer Data Protection Act of 2020 (CPA) (Wicker)	Public Health Emergency Privacy Act (PPA)(Blumenthal/Warner)	Differences Between the Two Bills
Covered Entities/ Organizations	<p>Any business subject to the FTC Act (plus common carriers and nonprofits) that collects, processes or transfers “covered data” or determines the means of collecting, processing or transferring “covered data.”</p> <p><u>Exclusions</u> A service provider.¹</p>	<p>Any entity (including a government entity) that (i) collects, uses, or discloses emergency health data electronically or by wire or radio; or (ii) that develops or operates a website or application for the purpose of contact tracing or otherwise responding to the COVID–19 PHE.</p> <p><u>Exclusions</u> (1) a health care provider²; (2) a person engaged in a de minimis collection or processing of emergency health data; (3) a service provider³; (d) a person acting in their individual or household capacity; or (e) a public health authority.</p> <p>Requirements do not apply to HIPAA covered entities and business associates, but within 30 days of enactment HHS is</p>	<p>CPA applies to HIPAA entities, but not to PHI. PPA does not apply to HIPAA entities, but requires HHS to issue guidance applying same requirements to HIPAA entities.</p> <p>CPA does not apply to service providers. PPA does not apply to service providers except those that operate websites or apps for COVID-19 purposes.</p> <p>CPA does not apply to government entities. PPA applies to government entities other than public health authorities.</p>

¹ A “service provider” is an entity that collects, processes or transfers covered data to perform services for a covered entity to which it is not related.

² “Health care provider” is defined as an “eligible health care provider” in Title VIII of division B of the CARES Act, which means “public entities, Medicare or Medicaid enrolled suppliers and providers, and such for-profit entities and not-for-profit entities not otherwise described in this proviso as the Secretary may specify, within the United States (including territories), that provide diagnoses, testing, or care for individuals with possible or actual cases of COVID– 19.”

³ A “service provider” is a person that receives, maintains, or transmits personal health information for the sole purpose to conduct business activities on behalf, for the benefit, and under instruction of the covered entity, but excludes a person that develops or operates a website or app for purposes of contact tracing or otherwise responding to the COVID–19 PHE.

		to issue guidance applying similar requirements to HIPAA covered entities and business associates, but must avoid duplication and not include a requirement if already required by HIPAA.	
Covered Data	<p>Precise geolocation data, proximity data, a persistent identifier⁴, and personal health information⁵ of an individual.</p> <p><u>Exclusions</u> (1) aggregated data, (2) business contact information,⁶ (3) de-identified data, (4) employee screening data⁷ and (5) publicly available information. Personal health information excludes protected health information (PHI) and education records subject to FERPA.</p> <p>An “individual” excludes an employee, owner, director, officer, staff member, trainee, vendor,</p>	<p>Emergency health data (“EHD”), which means data linked to or reasonably linkable to an individual or device that concerns the COVID–19 PHE. It includes geolocation, proximity, demographic, contact and any other data collected from a personal device.</p> <p><u>Exclusions</u> Manual contact tracing and case investigation by public health authorities or their agents.</p>	<p>CPA does not apply to business contact, or employment-related data. PPA does not exclude this data.</p> <p>CPA is not limited to data that concerns the COVID-19 PHI, but key provisions (e.g., notice affirmative express consent, data protection and minimization and public reporting) apply only during the COVID-19 PHE.</p>

⁴ A “persistent identifier” means a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time and across services and platforms, which may include a customer number held in a cookie, a static Internet Protocol (IP) address, a processor or device serial number, or another unique device identifier.

⁵ “Personal health information” means genetic information or information relating to the diagnosis or treatment of past, present, or future physical, mental health, or disability of the individual, and that identifies, or is reasonably linkable to, the individual.

⁶ “Business contact information” means information related to an individual’s business position name or title, business telephone number, business address, business email address, and other similar business information, provided that such information is collected, processed, or transferred solely for purposes related to such individual’s professional activities.

⁷ “Employee screening data” means data of employees or other personal collected, processed or transferred by a covered entity for purposes of determining, for purposes related to the COVID-19 public health emergency, whether the individual is permitted to enter a physical site of operation of the covered entity.

	visitor, intern, volunteer, or contractor of a covered entity permitted to enter a physical site of operation of the covered entity.		
Prohibited Uses and Disclosures		<p>May not disclose EHD to a government entity that is not a public health authority or for any purpose other than good faith public health purposes in direct response to exigent circumstances.</p> <p>May not collect, use or disclose EHD for a purpose not authorized by the bill, including (1) for commercial advertising and e-commerce; (2) for employment, finance, credit, insurance, housing, or education opportunities in a discriminatory manner or that otherwise makes opportunities unavailable on the basis of EHD or (3) segregating, discriminating or making unavailable places of public accommodation except for a lawful public health purpose.</p> <p>A government entity may not, and a covered organization may not knowingly facilitate the use of EHD to, or an individual's decision whether to participate in a program collecting EHD to, restrict, deny or interfere with an</p>	<p>AS long as affirmative express consent of individual is obtained, CPA has no explicit prohibitions. PPA prohibits use of EHD for unrelated purposes, including e-commerce, discrimination, or to interfere with voting rights.</p>

		<p>individual’s right to vote. Individual’s may bring a civil action in federal court for appropriate relief against a government entity that violates this prohibition.</p> <p>Does not prohibit public health or scientific research associated with the COVID–19 PHE by a public health authority, a 501(c)(3) nonprofit, an institution of higher education, or research, development, manufacture, or distribution of a drug, biological product, or vaccine that relates to a disease associated with the PHE.</p>	
Prior Notice and Consent	<p>During COVID-19 public health emergency (the “PHE”), covered entities must (obtain the individual’s affirmative consent to do for a covered purpose, and (3) publicly commit to not collecting, processing or transferring covered data for any purpose other than a covered purpose <u>unless</u> (1) necessary to comply with the bill or other applicable laws; (2) necessary to carry out operational or administrative tasks in support of a covered purpose; or (3) the individual gives affirmative express consent for that purpose.</p>	<p>Must obtain the individual’s prior affirmative express consent before collecting, using or disclosing EHD unless it is for the sole purpose of (i) protecting against malicious, fraudulent, or illegal activity; or to detect or respond to security incidents or threats; or (ii) if compelled to do so by a legal obligation</p>	<p>Both require affirmative express consent prior to collection of data, subject to limited exceptions. CPA exceptions are potentially a little broader in allowing use for operational or administrative tasks to support a covered purpose.</p>
Privacy Policy	<p>Within 14 days after enactment and during PHE, must publish a</p>	<p>Must provide a clear and conspicuous privacy notice at or prior to point</p>	

	<p>privacy policy and disclose it in a clear and conspicuous manner to an individual prior to or at point of collection of their covered data and to the public. Must include categories of recipients of covered data, and a description of the covered entity's retention and security practices.</p>	<p>of collection of EHD that explains purposes for which the data is collected, categories or recipients, the organization's data retention and security practices, how individuals may exercise their rights and how to contact the FTC to file a complaint.</p>	
<p>Public Reporting/ Reporting to Congress</p>	<p>During PHE, must provide a public report within 30 days of enactment and every 60 days thereafter of (1) the number of individuals in aggregate whose data it has collected, processed or transferred, (2) the categories of data collected, processed or transferred and the purposes for which each category of covered data was collected, processed or transferred, and (3) for transferred covered data, to whom it was transferred.</p>	<p>A covered organization that collects EHD of at least 100,000 individuals must provide a public report every 90 days of the number of individuals in aggregate terms whose data it has collected (to the extent practicable), the purposes for collection and the categories of third parties to whom disclosed</p> <p>HHS, in coordination with the US Commission on Civil Rights and the FTC must provide a report to Congress no sooner than 9 months or later than 12 months after enactment (and annually thereafter until 1 year after termination of the PHE) that examines the civil rights impact of the collection, use, and disclosure of health information in response to the COVID-19 PHE, including recommendations on preventing and addressing undue or disparate impact, segregation, discrimination, or infringements of civil</p>	<p>CPA requires public reporting without requirement for a minimum number of individuals. PPA requires reporting only if 100, 000 or more individuals are involved.</p> <p>CPA includes no reporting to Congress. The PPA requires annual reporting to Congress on the impact on civil rights until 1 year after the termination of the PHE.</p>

		rights in the collection and use of health information, including during a national health emergency.	
Consent Revocation	During the COVID-19 PHE, must permit the individual to revoke their consent and must stop collecting, processing or transferring the data for a covered purpose as soon as practicable but no later than within 14 days of receipt of the revocations or must de-identify it.	<p>Must provide an effective mechanism for an individual to revoke their consent and must stop collecting, using and disclosing their EHD as soon as practicable but no later than within 15 days after receipt of revocation.</p> <p>Must also destroy or render the EHD not linkable to the individual within 30 days of receipt of revocation. Must destroy EHD in a way that is impossible or demonstrably impracticable to identify the individual</p>	
Data Deletion	Must delete or de-identify the data when no longer used for a covered purpose or needed to comply with law or establish or defend a legal claim.	May not use or retain EHD after the later of (i) the end of the PHE declared by HHS; (ii) the end of a PHE declared by a state governor, or (iii) 60 days after collection. These requirements do not supersede requirements under the Privacy Act, HIPAA or other federal or state medical record retention, privacy or other requirements.	CPA does not provide explicit timeframes by which data must be deleted, whereas PPA requires deletion within 60 days of termination of the PHE or collection, whichever is later, but subject to record retention requirements of other laws.
Data Accuracy	Must take reasonable measures to ensure accuracy of covered data collected for a covered purpose and provide individuals with an effective mechanism to report inaccuracies.	Must take reasonable measures, where possible, to ensure the accuracy of EHD and provide an effective mechanism for an individual to correct inaccurate information	

Discrimination		Must adopt reasonable safeguards to prevent unlawful discrimination on the basis of EHD.	CPA has no explicit requirements regarding discrimination. The PPA prohibits use of data for unlawful discrimination and adoption of safeguards to prevent unlawful discrimination
Data Minimization	During PHE, must limit covered data collected, processed or transferred for a covered purpose to what is reasonably necessary, proportionate and limited to carry out that purpose. The FTC is to issue guidelines recommending best practices for this purpose within 30 days of enactment.	May only collect, use, or disclose EHD that is necessary, proportionate, and limited for a good faith public health purpose, including a service or feature to support that purpose.	
Security	During the PHE, covered entities must implement physical, technical and administrative safeguards to protect covered data	Must establish and implement reasonable data security policies, practices, and procedures to protect the security and confidentiality of emergency health data	
Enforcement	By FTC at an unfair or deceptive practice under the FTC Act, including against common carriers and Nonprofits. May also be enforced by State attorney generals (which may consolidate actions), but only if an FTC action is not pending, except if it involves violation of federal anti-discrimination laws, in which case the FTC will send the information to the appropriate state or federal authorities to initiate proceedings	By the FTC as an unfair or deceptive practice under the FTC Act, including against common carriers and nonprofits. May also be enforced by state attorney generals (or other state officers authorized under state law to bring actions), but they must first, where feasible, notify the FTC and allow it to intervene and may not bring an action if a FTC action is pending	
Private Right of Action		An individual may bring a civil action for	CPA has no private right of action, PPA does.

		<p>violations and the court may award between \$100-\$1000 per negligent violations and between \$500-\$5000 for reckless or intentional violations, as well as reasonable attorney fees, litigation costs and other appropriate relief. Any violation is deemed to be a concrete and particularized injury in fact.</p> <p>No pre-dispute arbitration agreement or pre-dispute joint action waiver will be valid or enforceable with respect to a dispute under the bill.</p>	
Preemption	<p>Preempts FCC regulations with respect to collection, processing or transfer of covered data for a covered purpose except with respect to 911 and emergency lines of hospitals, medical providers, fire departments or law enforcement.</p> <p>Also preempts state laws to the extent they relate to the collection, processing or transfer of covered data for a covered purpose</p>	<p>Does not preempt or supersede any Federal or State law or regulation, or limit the authority of the FTC or HHS under any other provision of law.</p>	<p>CPA preempts other related laws, PPA does not.</p>
Effective Date	<p>Upon enactment</p>	<p>Within 30 days of enactment (except as specified in the bill for specific regulations to be issued). In addition, upon enactment, but within 7 days after enactment the FTC must initiate, and with 45 days after enactment must complete, rulemaking to apply the same requirements to EHD collected by</p>	<p>CPA is prospective only, PPA would require regulations to apply the requirements to data collected before enactment to the extent practicable.</p>

		covered organizations before the date of enactment to the degree practicable.	
--	--	---	--



April 28, 2020

The Honorable Stephen M. Hahn, M.D.
Commissioner
U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20857

Dear Commissioner Hahn:

On behalf of the Confidentiality Coalition, thank you for addressing the important issue of modernizing the U.S. Food and Drug Administration's (FDA's) data strategy. Issues such as data stewardship, data exchange, data analytics and data quality are paramount to ensuring that the information gathered through various means both inside and outside of the healthcare system can be utilized in an appropriate, efficient manner to improve the well-being and health outcomes of individuals and populations.

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

The Confidentiality Coalition strongly supports an innovative healthcare system that harnesses data to elevate the quality of care delivery, turbocharges medical research, and enables greater efficiencies within the system. We are in a golden era of research and development, leading to treatments and technologies that are conquering disease and extending lives.

With this in mind, the Confidentiality Coalition's core approach to stewardship of healthcare data is that all care providers, health plans, and other entities that generate, hold, manage, exchange and share health data have a responsibility to take necessary steps to maintain the confidentiality and trust of patients and consumers. Our members believe that the framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules has proven an effective means of maintaining trust and accountability, and as such, it should be maintained.

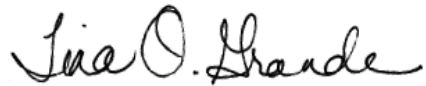
As you know, not all health information is protected under the HIPAA privacy and security rules. To safeguard individuals' health information when it is not protected under HIPAA, our members advocate for a national framework, based upon and harmonized with HIPAA, to establish a uniform approach for acceptable uses and disclosures of individually-identifiable health information. Attached to this letter is the Confidentiality Coalition's "Beyond HIPAA Privacy

The Honorable Stephen M. Hahn, M.D.
Page Two

Principles.” We encourage you to address data stewardship and modernizing the FDA’s data strategy through the lens of these principles.

In closing, we appreciate the opportunity to share with you these important principles that reflect the position of the Confidentiality Coalition’s membership, which spans all sectors of the healthcare system. We look forward to working with the FDA on issues related to data strategy and modernization. If you have any questions, please contact me at tgrande@hlc.org.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, looped initial "T".

Tina Olson Grande
Executive Vice President, Policy
Healthcare Leadership Council
On behalf of the Confidentiality Coalition

Enclosure(s)



CONFIDENTIALITY COALITION

MEMBERSHIP

AdvaMed	HITRUST
AdventHealth	Intermountain Healthcare
America's Health Insurance Plans	IQVIA
American Hospital Association	Johnson & Johnson
American Society for Radiation Oncology	Kaiser Permanente
AmerisourceBergen	Leidos
Amgen	Mallinckrodt
AMN Healthcare	Marshfield Clinic Health System
Anthem	Mayo Clinic
Ascension	McKesson Corporation
Association of American Medical Colleges	Medical Group Management Association
Association of Clinical Research Organizations	Medidata Solutions
athenahealth	Medtronic
Augmedix	MemorialCare Health System
Blue Cross Blue Shield Association	Millennium Health
BlueCross BlueShield of North Carolina	Memorial Sloan Kettering Cancer Center
BlueCross BlueShield of Tennessee	Merck
Cerner	MetLife
Change Healthcare	National Association of Chain Drug Stores
CHIME	National Community Pharmacists Association
Cigna	NewYork-Presbyterian Hospital
Ciox Health	NorthShore University HealthSystem
City of Hope	Pfizer
CLEAR	Pharmaceutical Care Management Association
Cleveland Clinic Foundation	Premier healthcare alliance
College of American Pathologists	SCAN Health Plan
ConnectiveRx	Senior Helpers
Cotiviti	SSM Health
CVS Health	State Farm
Datavant	Stryker
dEpid/dt Consulting Inc.	Surescripts
EMD Serono	Teladoc Health
Express Scripts	Texas Health Resources
Fairview Health Services	Tivity Health
Federation of American Hospitals	UCB
Genentech	UnitedHealth Group
Genetic Alliance	Vineti
Genosity	Vizient
Guardant	Workgroup for Electronic Data Interchange
Healthcare Leadership Council	ZS Associates
Health Management Systems	



Beyond HIPAA Privacy Principles

1. For the last 20 years, the HIPAA Privacy and Security Rules have engendered public trust that individually identifiable health information collected by providers and insurers (HIPAA covered entities) would be disclosed only for health functions like treatment, payment processing, and safety, and not used or disclosed for other purposes without an individual's authorization. Any future legislation or rulemaking that addresses individually identifiable health information should not conflict with HIPAA's Privacy and Security Rules.
 - a. HIPAA's required "Notice of Privacy Practices" provides an overview of individuals' rights as well as permitted and required uses and disclosures of identifiable health information.
 - b. HIPAA's approach requires use of risk-based administrative, technical, and physical safeguards allowing organizations the flexibility to implement policies and controls commensurate with the level of risks they have identified.
2. Congress should establish a single national privacy and security standard for *all* health information *not* subject to HIPAA. This single standard:
 - a. Should not conflict with HIPAA,
 - b. Should not disrupt day to day practices for HIPAA Covered Entities and Business Associates,
 - c. Should align with HIPAA's definitions of health information, and
 - d. Should adopt a risk-based approach like HIPAA.
3. Individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA Covered Entity or Business Associate Agreement are not afforded HIPAA privacy and security protections. Individuals should be given clear, succinct notice concerning collection, use, disclosure, and protection of individually identifiable health information that is not subject to HIPAA.
4. Individual authorization processes (including revocation of authorization) for use and disclosure of identifiable health information not covered by HIPAA should be written in a meaningful and understandable manner and should be easily accessible to individuals prior to and after information is used or shared.

5. Entities that hold or collect identifiable health information have a responsibility to take necessary steps to maintain the trust of individuals. Entities that are not HIPAA Covered Entities or Business Associates that hold identifiable health information should clearly stipulate the purposes for which they collect, use, and disclose identifiable health information.
6. Individuals must provide authorization for entities outside of HIPAA to collect individually identifiable health information. Such information collected, used or disclosed by entities outside of HIPAA should be limited to only that information needed to accomplish the purposes for data collection. This practice provides privacy protection while allowing for continued innovation.
7. Individuals should be informed of their right to seek redress – from the entity and from regulators – in the case of unauthorized access, misuse, or harm attributable to how their identifiable health information was collected, used or disclosed.
8. Penalties and enforcement must be meaningful in order to discourage misuse and unpermitted collection, use or disclosure of identifiable health information.

Privacy and Security Round Up

Apple-Google Contact Tracing System Pits Tech Giants Against Public Health Authorities

Following the Apple and Google [announcement](#) on April 10, 2020 of a joint initiative to enable the use of Bluetooth technology to help reduce the spread of COVID-19, there was considerable anticipation that this would be the contact tracing solution sought by public health authorities. The companies emphasized that user privacy and security would be “central to the design,” and their [description](#) of how an app would work noted that it would not require the sharing of user personal or location information. Thus, in an April 17, 2020 [opinion](#), the UK Information Commissioner stated that the initiative appeared to be “aligned with the principles of data protection by design and by default, including design principles around data minimization and security” and more European countries are [reported](#) to be embracing their approach. In contrast, several U.S. state and local public health authorities have raised concerns that the emphasis on privacy will come at the expense of public health, as the lack of location data will hamstring efforts to track and contain the spread of COVID-19. Some have also expressed cynicism at the tech giants’ concern about privacy when the data is collected for public health purposes, even as they and other tech companies amass user data for their own commercial purposes.

Comments: The Apple-Google initiative highlights the inherent tension between privacy and the public good. The need to strike the right balance between the privacy interests of individuals and the public good is also evident in recent bills introduced in Congress (see below), and comes as the Pew Research Center [reports](#) ambivalence and uncertainty by Americans, with 6 out of 10 not convinced that government collection of location data through cellphones will reduce the spread of COVID-19.

Republicans and Democrats Introduce Competing COVID-19 Privacy Bills

On May 14, 2020, Democratic Senators Blumenthal (D-CT) and Warner (D-VA) introduced the [Public Health Emergency Privacy Act](#), with a companion bill introduced in the House, to regulate the collection and use of data from consumers during the COVID-19 public health emergency (PHE). It follows the introduction of the [COVID-19 Consumer Protection Act of 2020](#) by Republican Senator Wicker (R-Miss) and others on May 7, 2020. Both bills require an individual’s affirmative express consent before collection of their data, clear and conspicuous privacy notices, data minimization, security measures, and data deletion when the data is no longer needed. However, the Democratic bill also includes several prohibitions, including on the use of the data to discriminate, interfere with voting rights, for commercial advertising and e-commerce, or by government agencies for purposes other than public health. While both bills have exclusions for data or entities subject to HIPAA, the Democratic bill would require the Department of Health and Human Services (HHS) to adopt similar requirements for HIPAA entities. The Republican bill also excludes business contact and employee data, whereas the Democratic bill does not. Enforcement for both would generally be by the FTC and state attorney generals, but the Democratic bill also includes a private right of action for individuals. Finally, while the Republican bill preempts other related laws, the Democratic bill does not.

Comments: While the bills reflect the usual partisan divide on preemption and private right of action, there is a substantial degree of commonality in their requirements. In addition, both bills would allow the collection and use of considerably more information than the Apple-Google construct. This, and the growing recognition that federal protections are a prerequisite to build the public trust needed to collect personal data for COVID-19 purposes, may finally provide the momentum for Congress to pass federal privacy legislation, albeit of limited scope.

OCR Issues Guidance on Media Disclosures During COVID-19 PHE

On May 3, 2020, the HHS Office of Civil Rights (OCR) issued [guidance](#) reminding covered health care providers that they may not give film crews and other media access to parts of their facilities where patients’ protected health information

(PHI) is accessible in any form without first obtaining a written HIPAA authorization from each patient. This is the case

even if the patients' identities are masked or blurred when airing the recorded video after the fact. Also, patients cannot be required to sign a HIPAA authorization as a condition of receiving treatment. Finally, even when HIPAA authorizations are obtained, covered health care providers must implement reasonable safeguards to protect the PHI of those patients who did not sign authorizations, such as installing computer monitor privacy screens to prevent film crews from viewing PHI on computers, and setting up opaque barriers to shield the PHI of non-authorizing patients.

Comments: The OCR Guidance is a reminder that access to PHI by the film crews themselves is an unauthorized disclosure unless HIPAA authorizations are obtained. There may be circumstances when a film crew could be acting as a business associate of the covered entity, in which case a business associate agreement rather than HIPAA authorizations would be required. But that would only be the case where the film crew is doing the filming as a service for the covered entity, such as for marketing the facility itself, and not for its own news reporting and even then, minimum necessary would apply and PHI could not be included in marketing materials without HIPAA authorizations.

FTC Solicits Comments on Health Breach Notification Rule

On May 8, 2020, the Federal Trade Commission (FTC) issued a Notice requesting comments on its 2009 Health Breach Notification Rule (Rule). This is part of the FTC's periodic review of its rules, which typically occurs every ten years, to ensure that the rules have kept up with changes in the marketplace, technology, and business models. The Rule requires personal health record (PHR) vendors, PHR-related entities (e.g. entities that provide apps that allow consumers to upload data into their PHRs) that are not covered by HIPAA to notify consumers, the FTC and, in some cases, the media, of a data breach. The FTC notes that only two breaches involving more than 500 individuals have been reported to it and that the FTC has not had to enforce the Rule because most PHR and related vendors have fallen under the HIPAA breach notification rule instead. However, the FTC notes that this may change with the proliferation of direct-to-consumer (DTC) health apps and similar technologies. Among other things, the FTC seeks comments on whether notifications under the Rule are at the right level, whether definitions or time frames should be changed, the implications for enforcement raised by DTC and similar technologies, and whether and how the Rule should address developments in health care products or services related to COVID-19. Comments will be accepted for 90 days after the notice is published in the Federal Register.

Comments: While the FTC review is part of its standard review process, it comes as a time of unprecedented flux in the type and purposes for which personal health data is collected directly from consumers, as well as a time of potential recalibration of the balance between privacy and public health interests. This, together with possible related Congressional action could portend more significant changes than might otherwise be the case.

Proposed California Rights Privacy Act Qualifies for November Ballot

On May 4, 2020, Californians for Consumer Privacy announced that it had obtained enough signatures to add the California Privacy Rights Act (CPRA) to the state's November 2020 ballot. The group's founder, Alastair Mactaggart, was instrumental in the passage of the California Consumer Privacy Act (CCPA), which went into effect January 1, 2020, and for which enforcement will begin July 1, 2020. The CPRA is intended to amend and expand the privacy rights in the CCPA in several ways, including adding a new category of "sensitive personal information subject to greater protections, adding a right to correct personal information that is inaccurate, increasing liability for data breaches, imposing much higher penalties for violations of children's privacy rights, and creating a new agency to enforce the law. These changes would be effective in 2023.

Comments: Some privacy advocates had strongly objected to the amendments made to the CCPA in 2019, believing that they went in the wrong direction. CPRA would include a provision limiting future amendments to those that further privacy rights unless there is another ballot initiative, thus preventing a "business onslaught" to weaken its protections. These developments come even as businesses await finalization of the California Attorney General's regulations implementing the CCPA. If nothing else, they make clear that California privacy laws are anything but settled.

Please contact Diane Sacks at dsacks@sacksllc.com or (202)459-2101 for more information on any of these items. This newsletter is intended to provide general information only and is not intended as legal advice.