



## **GENERAL COMMITTEE MEETING**

**Thursday, July 23, 2020  
3:00 PM to 4:00 PM**

### **Dial-In**

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

- 1. Welcome and Introductions**
- 2. Guest Speaker: Diane Sacks** Attachment 1, 2
  - a. TCPA Legal Developments/FCC-Anthem Decision**
- 3. Regulatory Update** Attachment 3, 4, 5, 6
  - a. 42 CFR Part 2 Final Rule**
  - b. OCR Rulemaking**
  - c. FTC Workshop Comments**
- 4. Legislative Update** Attachment 7, 8, 9
  - a. Telehealth**
  - b. Artificial Intelligence**
- 5. Monthly Privacy Round Up** Attachment 10
- 6. Articles of Interest** Attachment 11, 12, 13, 14

Next Meeting: September 17, 2020 3:00-4:00pm

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of
Rules and Regulations Implementing the
Telephone Consumer Protection Act of 1991
Anthem, Inc.
Petition for Declaratory Ruling and Exemption
CG Docket No. 02-278

DECLARATORY RULING AND ORDER

Adopted: June 25, 2020

Released: June 25, 2020

By the Chief, Consumer and Governmental Affairs Bureau:

I. INTRODUCTION

1. The Telephone Consumer Protection Act (TCPA) prohibits calls to wireless numbers made using an autodialer or an artificial or prerecorded voice unless the calls are "made for an emergency purpose or [are] made with the prior express consent of the called party." In 2015, health benefit company Anthem, Inc. (Anthem) filed a Petition for Declaratory Ruling and Exemption asking the Commission to exempt health plans and providers from the need to obtain prior express consent before making health care-related calls and text messages to wireless telephone numbers so long as they allow consumers to opt out of such messages after the fact. In other words, such health plan providers could enroll their customers in message programs without "prior express consent" and instead require consumers to take affirmative action to prevent such calls and text messages. Anthem also asks that the Commission exempt certain non-emergency, urgent health care-related calls from the requirements of the TCPA.

2. In this Declaratory Ruling and Order, we affirm that callers must get consumers' prior express consent before making autodialed calls or robocalls, and thus deny Anthem's requests.

II. BACKGROUND

3. In relevant part, the TCPA prohibits calls made using an autodialer or an artificial or prerecorded voice to wireless telephone numbers except when made: (1) for an emergency purpose; (2) with the prior express consent of the called party; (3) pursuant to a Commission-granted exemption; or (4) solely for the collection of a debt owed to or guaranteed by the United States. For the third of these exceptions, the TCPA gives the Commission the authority to exempt from the prior-express-consent

1 Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394, § 2(9) (1991), codified at 47 U.S.C. § 227(b)(1)(A); see also 47 CFR § 64.1200(a)(1).

2 See Petition of Anthem, Inc. for Declaratory Ruling and Exemption Regarding Non-Telemarketing Healthcare Calls, CG Docket No. 02-278, 1 (filed June 10, 2015) (Anthem Petition).

3 See id. at 3.

4 See 47 U.S.C. §§ 227(b)(1), (b)(2)(C); 47 CFR § 64.1200(a)(1). The Commission has concluded that the TCPA's protections apply to text messages as well as voice calls. See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14115, para. 165 (2003).

requirement only calls to wireless telephone numbers “that are not charged to the called party,” subject to conditions the Commission may prescribe “as necessary in the interest of the privacy rights [the TCPA] is intended to protect.”<sup>5</sup>

4. On June 10, 2015, Anthem filed a petition asking the Commission to clarify that the TCPA’s prior-express-consent requirement does not apply to its calls. Anthem asks us to exempt health care plans and providers from the need to obtain prior express consent before making health care-related calls and text messages to wireless telephone numbers so long as they allow consumers to opt out after the fact.<sup>6</sup> Anthem also asks us to exempt certain non-emergency, health care-related calls that are purportedly “urgent” from the requirements of the TCPA.<sup>7</sup> Anthem characterizes these “specific calls and texts” as case management calls, preventative medicine calls, and calls regarding the use and maintenance of medical benefits.<sup>8</sup> Anthem makes several policy arguments as well, including that the calls benefit consumers, are welcomed by consumers, and are otherwise regulated, which it asserts should allay any TCPA-related concerns.<sup>9</sup>

5. The Consumer and Governmental Affairs Bureau (Bureau) sought comment on the Anthem Petition.<sup>10</sup> Four commenters, including health care providers, national retail drug store chains, and a health benefits coordinator, filed comments supporting Anthem.<sup>11</sup> These commenters argue that the Commission should exempt from the TCPA’s prior-express-consent requirement the calls Anthem identifies because they have the potential to “improve medical treatment compliance, medication adherence and appointment attendance.”<sup>12</sup> One consumer filed an *ex parte* comment opposing the petition, asserting that Anthem’s calls are not “emergency” calls and that content-based exemptions to the TCPA are not appropriate.<sup>13</sup>

6. On March 20, 2020, the Bureau, in response to the COVID-19 pandemic, issued a declaratory ruling offering clarification regarding “emergency purposes” calls and the TCPA.<sup>14</sup> The Bureau clarified that government officials and public health care authorities, as well as a person under the

---

<sup>5</sup> 47 U.S.C. § 227(b)(2)(C). We note that Anthem’s petition neglects to cite this statutory basis for the requested Commission action.

<sup>6</sup> See Anthem Petition at 12-14.

<sup>7</sup> See *id.* at 14-17.

<sup>8</sup> See *id.*

<sup>9</sup> See *id.* at 3-12.

<sup>10</sup> *Consumer and Governmental Affairs Bureau Seeks Comment on Petition for Declaratory Ruling Filed by Anthem, Inc.*, CG Docket No. 02-278, Public Notice, 30 FCC Rcd 9774 (2015).

<sup>11</sup> Adventist Health System Comments (rec. Sept. 30, 2015) (Adventist Comments); WellCare Health Plans, Inc. Comments (rec. Sept. 30, 2015) (WellCare Comments); CVS Health Corporation and Rite Aid Hdqtrs. Corp. Comments (rec. Sept. 30, 2015) (CVS Comments); United Healthcare Services, Inc. Comments (rec. Sept. 30, 2015) (UHS Comments).

<sup>12</sup> Adventist Comments at 2; see also CVS Comments at 7; UHS Comments at 5.

<sup>13</sup> See Letter from Roger Biggerstaff to Marlene H. Dortch, Secretary, FCC, CG Docket No. 02-278, at 3 (filed Oct. 16, 2015).

<sup>14</sup> See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Declaratory Ruling, 35 FCC Rcd 2840 (CGB 2020) (*COVID-19 Declaratory Ruling*); see also Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak (Mar. 13, 2020), <https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/>; 47 CFR § 64.1200(f)(4) (defining “emergency purposes” as “calls made necessary in any situation affecting the health and safety of consumers”).

express direction of such an organization and acting on its behalf, can make automated calls directly related to the health or safety risks arising out of the COVID-19 outbreak pursuant to the TCPA's "emergency purpose" exception.<sup>15</sup> Such emergency calls are permissible under the TCPA and the Commission's implementing rules even without the prior express consent of the called party.

### III. DISCUSSION

7. In this Order, we affirm that makers of robocalls generally must obtain a consumer's prior express consent *before* making calls to the consumer's wireless phone number.<sup>16</sup> And we note that, to the extent that calls are welcomed by consumers, callers should be able to easily obtain prior express consent for them.

8. Congress was clear in enacting the TCPA that consumers should be protected from unwanted robocalls.<sup>17</sup> Consumers consistently tell the Commission that unwanted calls are their top concern, a fact that prompted recent enactment of the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED) Act.<sup>18</sup> For wireless calls, the TCPA contains clear, specific exceptions for the narrow set of calls consumers are likely to want to receive—such as emergency calls—but does not authorize a broad exception for health care-related calls. We therefore reiterate the statutory requirement that callers must obtain consumers' *prior* express consent for such calls and may not instead require consumers to affirmatively opt out of them after the fact.<sup>19</sup>

9. In reaching our conclusion, we reject Anthem's various arguments. We disagree that health care-related wireless calls should be exempt from the prior-express-consent requirement so long as consumers are allowed to opt out because there is a pre-existing relationship between the consumer and the caller (the consumer's health care provider or health care plan) that constitutes consent.<sup>20</sup> The mere existence of a caller-consumer relationship does not satisfy the prior-express-consent requirement for

---

<sup>15</sup> See *COVID-19 Declaratory Ruling*, 35 FCC Rcd at 2841-42, paras. 6-8.

<sup>16</sup> We reiterate that there is no general exception to the prior-express-consent requirement for health care-related calls but note that in 2015 the Commission adopted a limited exemption to the requirement for certain health care-related calls when they are, among other things, free to the end user. See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, WC Docket No. 07-135, Declaratory Ruling and Order, 30 FCC Rcd 7961, 8031-32, paras. 147-48 (2015) (*2015 TCPA Declaratory Ruling and Order*).

<sup>17</sup> See Pub. L. No. 102-243, § 2(9) (1991).

<sup>18</sup> See Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019).

<sup>19</sup> The Commission has clarified that "persons who knowingly release their phone numbers" for a particular purpose "have in effect given their invitation or permission to be called at the number" for that purpose "absent instructions to the contrary." *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 92-90, Report and Order, 7 FCC Rcd 8752, 8769, para. 31 (1992) (*1992 TCPA Order*). The Commission has examined the issue of prior express consent in the context of health care-related calls: "[T]he provision of a phone number to a healthcare provider constitutes prior express consent for healthcare calls subject to HIPAA . . . if the covered entities and business associates are making calls within the scope of consent given, and absent instructions to the contrary." *2015 TCPA Declaratory Ruling and Order*, 30 FCC Rcd 8020, para. 141. The Commission further clarified that "within the scope of consent given" means "the call must be closely related to the purpose for which the telephone number was originally provided." *Id.* at 8020 n.474.

<sup>20</sup> See Anthem Petition at 2, 13.

calls to wireless numbers, nor does it create an exception to this requirement.<sup>21</sup>

10. We also reject Anthem’s request that we exempt certain non-emergency, health care-related calls that it claims are “urgent” from the requirements of the TCPA. Anthem cites no statutory authority to support its request that we create an “urgent circumstances” exemption.<sup>22</sup> Further, we are skeptical that the types of calls Anthem would make under such an exception would reasonably be considered “urgent” by consumers. For example, calls to “educate members about available services and benefits” are not likely to be so time-sensitive and critical to justify bypassing consumer consent.<sup>23</sup> And unlike the automated calls concerning the COVID-19 pandemic we addressed in our recent *COVID-19 Declaratory Ruling*, the calls Anthem describes do not appear to be “made necessary by incidents of imminent danger including ‘health risks’ affecting health and safety.”<sup>24</sup> Such calls therefore are not made for an “emergency purpose” as defined by the Commission’s rules.<sup>25</sup> We note, however, that to the extent any calls covered by Anthem’s petition would meet the criteria set forth in the recent *COVID-19 Declaratory Ruling*, such calls would be governed by that Declaratory Ruling and hence would not require prior express consent.

11. We also reject Anthem’s suggestion that health care-related calls from health plans and providers to wireless telephones should be exempt from the TCPA’s prior-express-consent requirement because such calls are welcomed by consumers. The TCPA gives the Commission authority to only exempt specific, limited types of calls to wireless phone numbers from the prior-express-consent requirement; even in those narrow circumstances, whether those calls are welcomed by consumers has not

---

<sup>21</sup> To the extent Anthem is asking us to find an established business relationship exception applies to its calls, we do not find reason to do so. Congress could have included an explicit established business relationship exception for calls to wireless numbers in the TCPA (as it did in the case of faxes) but it did not, nor did Congress give the Commission the authority to adopt an established business relationship exception for *wireless* calls on the grounds that such calls do not “adversely affect [consumer] privacy rights,” which the TCPA does provide for calls to *residential* lines. 47 U.S.C. 227(b)(2)(B)(ii)(I); *see also* 1992 TCPA Order, 7 FCC Rcd at 8770, para. 34; *Rules and Regulations Implementing the Telephone Consumer Protection Act*, CG Docket No. 02-278, Report and Order, 27 FCC Rcd 1830, 1845, para. 35 n.102 (2012) (*2012 TCPA Order*); 47 CFR § 64.1200(a)(4)(i).

<sup>22</sup> To the extent Anthem’s “urgent circumstances” request is grounded in the Commission’s authority to “by rule or order, exempt from the [TCPA’s restrictions on calls to wireless numbers made using an autodialer or a prerecorded or artificial voice] calls to a telephone number assigned to a cellular telephone service that are not charged to the called party, subject to such conditions as the Commission may prescribe as necessary in the interest of the privacy rights this section is intended to protect,” it also fails. 47 U.S.C. § 227(b)(2)(C). For example, Anthem has not argued it could satisfy the provision’s minimal factual requirements, including that the calls would be free to the end user. *See id.* (“calls to a telephone number assigned to a cellular telephone service that are not charged to a called party”). To the extent that the calls Anthem wishes to make fall within the parameters set forth in the *2015 TCPA Declaratory Ruling and Order*, the exemption granted therein for certain health care-related calls could apply. *See 2015 TCPA Declaratory Ruling and Order*, 30 FCC Rcd at 8030-32, paras. 143-48.

<sup>23</sup> *See* Anthem Petition at 16.

<sup>24</sup> *COVID-19 Declaratory Ruling*, 35 FCC Rcd at 2841-42, paras. 6-8 (citing *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Blackboard, Inc. Petition for Expedited Declaratory Ruling*, CG Docket No. 02-278, Declaratory Ruling, 31 FCC Rcd 9054, 9063, para. 21 (2016) (concluding that calls or messages relating to weather closures, incidents of threats and/or imminent danger to the school due to fire, dangerous persons, health risks, and unexcused absences constitute calls made for an emergency purpose because they potentially affect the health and safety of students and faculty)).

<sup>25</sup> *See* 47 CFR § 64.1200(f)(4) (defining “emergency purposes” to mean “calls made necessary in any situation affecting the health and safety of consumers”).

previously been part of our inquiry.<sup>26</sup> Moreover, if these calls are in fact popular with consumers, as Anthem argues, consumers should be willing to give their prior express consent for them.<sup>27</sup> The ways Anthem can obtain prior express consent for these calls are numerous and not particularly arduous, especially where there already is a relationship with the consumer.

12. Finally, we reject Anthem's argument that a TCPA exemption for health care-related calls made by health care plans and providers to wireless telephone numbers will not result in abuse because patient outreach is already subject to a strict regulatory regime under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule. The TCPA contains no exception to the prior-express-consent requirement for calls to wireless phone numbers if those calls are also regulated by other laws. HIPAA regulates the content of communications (to ensure the privacy of patient information) whereas the TCPA regulates the methodology of the communication (to restrict calls and texts made using an autodialer or an artificial or prerecorded voice, and made without the prior express consent of the called party).<sup>28</sup> A call that complies with HIPAA requirements does not necessarily comply with TCPA requirements or satisfy that statute's legislative goals.

#### IV. ORDERING CLAUSE

13. Accordingly, IT IS ORDERED pursuant to sections 1-4 and 227 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 227, sections 1.2 and 64.1200 of the Commission's Rules, 47 CFR §§ 1.2, 64.1200, and the authority delegated in sections 0.141 and 0.361 of the rules, 47 CFR §§ 0.141, 0.361, that the Petition for Declaratory Ruling and Exemption filed by Anthem, Inc. in CG Docket No. 02-278 on June 10, 2015, IS DENIED.

14. IT IS FURTHER ORDERED that this Declaratory Ruling and Order shall be effective upon release.

FEDERAL COMMUNICATIONS COMMISSION

Patrick Webre  
Chief  
Consumer and Governmental Affairs Bureau

<sup>26</sup> The Commission has the authority to and did grant a limited exemption for health care-related calls in 2015. *See* 47 U.S.C. § 227(b)(2)(C); *see also* 2015 TCPA Declaratory Ruling and Order, 30 FCC Rcd at 8031-32, paras. 146-48. In order for such calls to be exempt from the TCPA's consent requirement they must be exigent and have a health care treatment purpose, as well as meet a number of conditions including, but not limited to, being free to the end user. Anthem has not asserted, let alone proven, that it will meet these criteria. The purported popularity of the call is not part of our exemption inquiry.

<sup>27</sup> Anthem's Petition is inherently contradictory. On the one hand, Anthem spends the majority of its petition asserting that these calls are not only beneficial to, but also welcomed by consumers. On the other hand, Anthem alleges, without any evidence, that it is difficult to obtain consent for the calls it wishes to make. *See* Anthem Petition at 9. Even if Anthem's latter allegation is correct and it is difficult to obtain consent, this provides no basis as a matter of law for an exception to or the creation of an exemption from the TCPA's consent requirement.

<sup>28</sup> *See* 2012 TCPA Order, 27 FCC Rcd at 1852, para. 57 (describing the "privacy protections" of HIPAA, in part, as "giv[ing] individuals important controls over whether and how their protected information is used and disclosed for marketing purposes" and "requir[ing] an individual's written authorization before his or her protected health information can be used or disclosed for marketing purposes"); *see also* 47 USC § 227(b)(1).

# Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule

The 42 CFR Part 2 regulations (Part 2) serve to protect patient records created by federally assisted programs for the treatment of substance use disorders (SUD). Part 2 has been revised to further facilitate better coordination of care in response to the opioid epidemic while maintaining its confidentiality protections against unauthorized disclosure and use.

**What Has Not Changed Under the New Part 2 Rule:** The revised rule does not alter the basic framework for confidentiality protection of substance use disorder (SUD) patient records created by federally assisted SUD treatment programs. Part 2 continues to prohibit law enforcement's use of SUD patient records in criminal prosecutions against patients, absent a court order. Part 2 also continues to restrict the disclosure of SUD treatment records without patient consent, other than as statutorily authorized in the context of a bona fide medical emergency; or for the purpose of scientific research, audit, or program evaluation; or based on an appropriate court order.

**What Has Changed Under the New Part 2 Rule:** The revised rule modifies several major sections of Part 2, as follows:

Provision	What Changed?	Why Was This Changed?
<b>Applicability and Re-Disclosure</b>	Treatment records created by non-Part 2 providers based on their own patient encounter(s) are explicitly not covered by Part 2, unless any SUD records previously received from a Part 2 program are incorporated into such records. Segmentation or holding a part of any Part 2 patient record previously received can be used to ensure that new records created by non-Part 2 providers will not become subject to Part 2.	To facilitate coordination of care activities by non-part-2 providers.
<b>Disposition of Records</b>	When an SUD patient sends an incidental message to the personal device of an employee of a Part 2 program, the employee will be able to fulfill the Part 2 requirement for "sanitizing" the device by deleting that message.	To ensure that the personal devices of employees will not need to be confiscated or destroyed, in order to sanitize in compliance with Part 2.
<b>Consent Requirements</b>	An SUD patient may consent to disclosure of the patient's Part 2 treatment records to an entity (e.g., the Social Security Administration), without naming a specific person as the recipient for the disclosure.	To allow patients to apply for benefits and resources more easily, for example, when using online applications that do not identify a specific person as

Provision	What Changed?	Why Was This Changed?
		the recipient for a disclosure of Part 2 records.
<b>Disclosures Permitted w/ Written Consent</b>	Disclosures for the purpose of “payment and health care operations” are permitted with written consent, in connection with an illustrative list of 18 activities that constitute payment and health care operations now specified under the regulatory provision.	In order to resolve lingering confusion under Part 2 about what activities count as “payment and health care operations,” the list of examples has been moved into the regulation text from the preamble, and expanded to include care coordination and case management activities.
<b>Disclosures to Central Registries and PDMPs</b>	<p>Non-OTP (opioid treatment program) and non-central registry treating providers are now eligible to query a central registry, in order to determine whether their patients are already receiving opioid treatment through a member program.</p> <p>OTPs are permitted to enroll in a state prescription drug monitoring program (PDMP), and permitted to report data into the PDMP when prescribing or dispensing medications on Schedules II to V, consistent with applicable state law.</p>	To prevent duplicative enrollments in SUD care, duplicative prescriptions for SUD treatment, and adverse drug events related to SUD treatment.
<b>Medical Emergencies</b>	Declared emergencies resulting from natural disasters (e.g., hurricanes) that disrupt treatment facilities and services are considered a “bona fide medical emergency,” for the purpose of disclosing SUD records without patient consent under Part 2.	To ensure clinically appropriate communications and access to SUD care, in the context of declared emergencies resulting from natural disasters.
<b>Research</b>	Disclosures for research under Part 2 are permitted by a HIPAA-covered entity or business associate to individuals and organizations who are neither HIPAA covered entities, nor subject to the Common Rule (re: Research on Human Subjects).	To facilitate appropriate disclosures for research, by streamlining overlapping requirements under Part 2, the HIPAA Privacy Rule and the Common Rule.
<b>Audit and Evaluation</b>	Clarifies specific situations that fall within the scope of permissible disclosures for audits and/or program evaluation purposes.	To resolve current ambiguity under Part 2 about what activities are covered by the audit and evaluation provision.



<b>Provision</b>	<b>What Changed?</b>	<b>Why Was This Changed?</b>
<b>Undercover Agents and Informants</b>	Court-ordered placement of an undercover agent or informant within a Part 2 program is extended to a period of 12 months, and courts are authorized to further extend the period of placement through a new court order.	To address law enforcement concerns that the current policy is overly restrictive to some ongoing investigations of Part 2 programs.

## RIN Data

**HHS/OCR**

**RIN:** 0945-AA00

**Publication ID:** Spring 2020

**Title:** HIPAA Privacy: Changes To Support, and Remove Barriers to, Coordinated Care and Individual Engagement

**Abstract:**

This proposed rule would seek comment on proposals to modify provisions of the HIPAA Rules that may impede the transformation of the health care system to value-based health care, by limiting or discouraging care coordination and case management (including care coordination challenges arising from the opioid crisis) among hospitals, physicians (and other providers), payors, and patients. The proposals would decrease unnecessary compliance burdens, while continuing to protect the privacy and security of individuals' protected health information (PHI). The proposed modifications also would support (and remove barriers to) the engagement of individuals with the healthcare system by strengthening individuals' ability to access their PHI.

**Agency:** Department of Health and Human Services(HHS)

**Priority:** Other Significant

**RIN Status:** Previously published in the Unified Agenda

**Agenda Stage of Rulemaking:** Proposed Rule Stage

**Major:** Yes

**Unfunded Mandates:** No

**EO 13771 Designation:** Deregulatory

**CFR Citation:** [45 CFR 164](#)

**Legal Authority:** [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\) Pub. L. 104-191, sec. 264.](#) [Health Information Technology for Economic and Clinical Health \(HITECH\) Act, Pub. L. 115-5, sec. 13405.](#)

**Legal Deadline:** None

**Timetable:**

	Action	Date	FR Cite
RFI		11/01/2018	<a href="#">83 FR 64302</a>
RFI Comment Period End		02/19/2019	
NPRM		06/00/2020	

**Regulatory Flexibility Analysis Required:** No

**Government Levels Affected:** Federal, Local, State, Tribal

**Small Entities Affected:** No

**Federalism:** No

**Included in the Regulatory Plan:** Yes

**RIN Information URL:** [www.hhs.gov/ocr/privacy](http://www.hhs.gov/ocr/privacy)

**RIN Data Printed in the FR:** No

**Agency Contact:**

Marissa Gordon-Nguyen  
Senior Advisor for Health Information  
Department of Health and Human Services  
Office for Civil Rights  
200 Independence Avenue SW,  
Washington, DC 20201  
Phone:800 368-1019  
TDD Phone:800 537-1697  
Email: ocrprivacy@hhs.gov

## RIN Data

HHS/OCR

RIN: 0945-AA04

Publication ID: Spring 2020

**Title:** HIPAA Enforcement and Privacy Rules: Annual Penalty Limits and Sharing Civil Money Penalties or Monetary Settlements With Harmed Individuals and Accounting of Disclosures Under the HITECH Act

**Abstract:**

This proposed rule would solicit the public's views on proposals to modify the HIPAA Enforcement Rule by adjusting some annual limits on CMPs under the HITECH Act and establishing a methodology for the distribution of civil money penalties and monetary settlements with those harmed by an offense under HIPAA relating to privacy or security. It also would propose to modify the HIPAA Privacy Rule as necessary to implement the accounting of disclosures provisions of section 13405(c) of the Health Information Technology for Economic and Clinical Health Act (title XIII of the American Recovery and Reinvestment Act of 2009). We plan to withdraw the current Accounting of Disclosures NPRM that was issued in 2011 when the new NPRM is issued.

**Agency:** Department of Health and Human Services(HHS)

**Priority:** Other Significant

**RIN Status:** Previously published in the Unified Agenda

**Agenda Stage of Rulemaking:** Proposed Rule Stage

**Major:** No

**Unfunded Mandates:** No

**EO 13771 Designation:** Other

**CFR Citation:** [45 CFR 160](#) [45 CFR 164](#)

**Legal Authority:** [Health Information Technology for Economic and Clinical Health \(HITECH\) Act, Pub. L. 111-5, sec. 13410\(c\)\(3\) & \(4\)](#) Social Security Act, sec. 1776 [42 U.S.C. 1320d-5, as amended by HITECH Act sec. 13410\(a\), \(d\), and \(f\)](#) [PL 111-5, sec 13405\(c\)](#)

**Legal Deadline:**

Action	Source	Description	Date
Final	Statutory	The statutory deadline for issuing a rule on sharing of civil monetary penalties or monetary settlements was 2/17/2012.	02/17/2012
Final	Statutory	Issuing a rule on Accounting of Disclosures is statutory not later than 6 months after the Secretary adopts standards on accounting of disclosures described in HITECH section 13101.	06/01/2010

**Overall Description of Deadline:** The statutory deadline to issue a rule on the requirements on the sharing of civil monetary penalties (CMP) or monetary settlements with individuals harmed by the actions for which CMPs were imposed was February 17, 2012, pursuant to the HITECH Act. Issuing a rule on Accounting of Disclosures is statutory not later than 6 months after the Secretary adopts standards on accounting of disclosures described in HITECH section 13101.

**Timetable:**

Action	Date	FR Cite
NPRM	05/31/2011	<a href="#">76 FR 31426</a>
NPRM Comment Period End	08/01/2011	
Second NPRM	04/00/2021	

**Regulatory Flexibility Analysis Required:** No

**Government Levels Affected:** None

**Small Entities Affected:** No

**Federalism:** No

**Included in the Regulatory Plan:** No

**RIN Information URL:** [www.hhs.gov/ocr/privacy](http://www.hhs.gov/ocr/privacy)

**RIN Data Printed in the FR:** No

**Agency Contact:**

Marissa Gordon-Nguyen  
Senior Advisor for Health Information  
Department of Health and Human Services  
Office for Civil Rights  
200 Independence Avenue SW,  
Washington, DC 20201  
Phone:800 368-1019  
TDD Phone:800 537-1697  
Email: ocrprivacy@hhs.gov



**FEDERAL TRADE COMMISSION**  
PROTECTING AMERICA'S CONSUMERS

# Data To Go: An FTC Workshop on Data Portability

SEP 22, 2020 9:00AM–5:00PM

**CONSTITUTION CENTER**

400 7th St SW, Washington, DC 20024 | [Directions & Nearby](#)

Constitution Center Auditorium

**TAGS:** [Bureau of Consumer Protection](#) | [Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#)

## Event Description

The Federal Trade Commission will host a public workshop on September 22, 2020, to examine the potential benefits and challenges to consumers and competition raised by data portability.

Data portability refers to the ability of consumers to move data – such as, emails, contacts, calendars, financial information, health information, favorites, friends or content posted on social media – from one service to another or to themselves. In addition to providing benefits to consumers, data portability may benefit competition by allowing new entrants to access data they otherwise would not have so that they can grow competing platforms and services. At the same time, there may be challenges to implementing or requiring data portability. For example, data that consumers want to port may include information about others, such as friends' photos and comments. How should this data be treated? How can the data be transferred securely? Who has responsibility for ensuring that data portability is technically feasible? Does mandatory data access or data sharing affect companies' incentives to invest in data-driven products and services?

Data portability is a timely topic. Europe's General Data Protection Regulation and California's Consumer Privacy Act both include data portability requirements, and companies serving customers in Europe and California have already begun providing consumers with the right to port their data. In addition, the UK's Open Banking initiative and US banking laws requiring that financial information be provided to consumers in an electronic format, are encouraging data portability in the financial sector, including the development of APIs to facilitate transfer of data to consumers and among financial institutions. Major technology companies Apple, Facebook, Google, Microsoft, and Twitter have created the Data Transfer Project with the goal of creating an open-source, service-to-service data portability platform. The Department of Health and Human Services' Office of National Coordinator for Health Information Technology has finalized rules to facilitate portability of health data. And industry and lawmakers have discussed including data portability as a component of any comprehensive federal privacy legislation.

The workshop seeks to bring together stakeholders — including industry representatives, economists, consumer advocates, and regulators — for a wide-ranging public discussion on issues raised by data portability. The workshop will address questions such as the potential benefits to consumers and competition of data portability, the potential risks to

## Attachment #6

consumer privacy and how those risks might be mitigated, the potential impact of mandatory data access or data sharing on companies' incentives to innovate, how to best ensure the security of personal data that is being transmitted from one business to another, the merits and challenges of interoperability, and who should be responsible for ensuring interoperability.

To help assist the agency's analysis of this topic, the FTC is seeking comment on a range of issues including:

- How are companies currently implementing data portability? What are the different contexts in which data portability has been implemented?
- What have been the benefits and costs of data portability? What are the benefits and costs of achieving data portability through regulation?
- To what extent has data portability increased or decreased competition?
- Are there research studies, surveys, or other information on the impact of data portability on consumer autonomy and trust?
- Does data portability work better in some contexts than others (e.g., banking, health, social media)? Does it work better for particular types of information over others (e.g., information the consumer provides to the business vs. all information the business has about the consumer, information about the consumer alone vs. information that implicates others such as photos of multiple people, comment threads)?
- Who should be responsible for the security of personal data in transit between businesses? Should there be data security standards for transmitting personal data between businesses? Who should develop these standards?
- How do companies verify the identity of the requesting consumer before transmitting their information to another company?
- How can interoperability among services best be achieved? What are the costs of interoperability? Who should be responsible for achieving interoperability?
- What lessons and best practices can be learned from the implementation of the data portability requirements in the GDPR and CCPA? Has the implementation of these requirements affected competition and, if so, in what ways?

Comments may be submitted until August 21, 2020 electronically to [DataPortability@ftc.gov](mailto:DataPortability@ftc.gov). If you prefer to file your comment on paper, write "FTC Data Portability Workshop" on your comment and on the envelope and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th St., SW, 5th Floor, Suite 5610, Washington, DC 20024.

## Event Details

---

### ABOUT THIS VENUE

---

## FTC Privacy Policy

Under the Freedom of Information Act ("FOIA") or other laws, we may be required to disclose to outside organizations the information you provide when you pre-register. The Commission will consider all timely and responsive public comments, whether filed in paper or electronic form, and as a matter of discretion, we make every effort to remove home contact information for individuals from the public comments before posting them on the FTC website.



# WAYS AND MEANS

REPUBLICANS | KEVIN BRADY, REPUBLICAN LEADER

## DISCUSSION DRAFT:

### Keeping Medicare Patients' Improved Access to Care through Telehealth

Amidst the coronavirus pandemic, Congress and the Administration have enacted unprecedented expansions to telehealth in the Medicare program. [According to the Centers for Medicare and Medicaid Services \(CMS\)](#), over the course of the first three months of this crisis, over 9 million beneficiaries utilized telehealth, and the nation went from 13,000 Medicare beneficiaries accessing telehealth services over the course of an average week to an estimated 1.7 million per week.<sup>1</sup> This is a massive increase. Patients and stakeholders now wonder whether these temporary waivers will be a part of the future of telehealth in Medicare. This discussion draft aims to serve as a starting point for that conversation.

#### **Sec. 2- Make Telehealth Convenience Permanent: Patients should be able to continue to use telehealth services at home**

Traditionally, in order to receive a telehealth service in Medicare, a beneficiary must be in a rural area and must travel to a health care facility. By removing geographic and originating site restrictions, Medicare beneficiaries across the country will have the permanent option of utilizing telehealth services from the convenience of their home.

#### **Sec. 3- Permanently lift restrictions on Federally Qualified Health Centers (FQHCs) and Rural Health Clinics (RHCs) to improve access for rural and underserved Medicare patients.**

Prior to the Public Health Emergency waivers, FQHCs and RHCs were restricted in their ability to provide telehealth services to Medicare beneficiaries. Permanently removing these restrictions is critical to improving access for patients in rural and underserved areas.

#### **Sec. 4- Permanently allow certain clinical practitioners (physical therapists, speech pathologists, occupational therapists) to give care via telehealth, and give the Secretary of Health and Human Services (HHS) the authority to waive limitations on other types of clinical practitioners.**

Waiver expansions during the pandemic opened up access to care and broadened the previously narrow list of providers that were eligible to furnish telehealth. Breaking down these limitations to telehealth services in Medicare will help patients access care.

---

<sup>1</sup> "Early Impact Of CMS Expansion Of Medicare Telehealth During COVID-19," Health Affairs Blog, July 15, 2020. DOI: 10.1377/hblog20200715.454789

**Sec. 5- Permanently allow telehealth services through audio-only telephone, when audio-visual isn't an option and if the patient and provider have an established relationship.**

Audio-only telehealth has been critical for reaching many patients that otherwise might not be able to receive care during the pandemic. Many patients have limited access to video-conferencing, whether because of poor infrastructure in rural and underserved areas or limited digital literacy. While we study how to best incorporate audio-only telehealth, it is clear this option has helped and should remain a tool for patients and providers.

**Sec. 6- Permanently allow Health Saving Account (HSA)-eligible plans to cover telehealth services before meeting the plan's deductible**

Making this policy permanent will give the 22 million Americans with HSAs easier access to this effective and convenient type of care, potentially lowering health care costs overall.

**Sec. 7- Permanently allow the remote authorization of dialysis care through telehealth technologies instead of requiring an in-person visit.**

The Public Health Emergency (PHE) has demonstrated the ability to better integrate telehealth into a variety of home health settings. Moving forward, patients should have the choice to continue to use telehealth to receive care such as home dialysis, **so long as patients receive mandatory in-person training when they start home dialysis**. Additionally, the Secretary of HHS should have the ability to expand similar flexibilities to other cases **by waiving other in-person visit requirements**, where clinically appropriate and safe.

Program Integrity:

**Sec. 8- Requires the HHS Office of the Inspector General to conduct a survey of telehealth claims to study potential improper payments 1 year after the end of the PHE.**

**Sec. 9- Increases funding to the HHS Office of Audit Services and Office of Investigations to ensure oversight of the increase in telehealth claims since the start of the pandemic.**

**Sec. 10- Requires CMS to offer education and training sessions to practitioners on Medicare telehealth requirements and related resources.**

Increasing patients' opportunity to utilize telehealth should not result in increasing waste, fraud, and abuse. Any steps Congress takes to expand telehealth must also include appropriate program integrity safeguards.

JULY 20,2020

## Wyden Proposes Major Expansion of Telehealth in Medicare

*New Legislation from Finance Committee Ranking Member is Largest Improvement to Telehealth in Decades*

*Bill Includes Removal of Restrictions for Non-Rural Areas, Access to Mental Health Care Via Telehealth for All Seniors in Medicare*

**Washington, D.C.** – Senate Finance Committee Ranking Member Ron Wyden, D-Ore., today released a proposal to significantly expand the availability of telehealth services in Medicare on a permanent basis. The bill comes as the use of telehealth services has greatly increased during the COVID-19 pandemic, offering a safe option for at-risk populations.

**“Out of necessity during this pandemic, doctors, patients and public health officials have come to recognize that telehealth works,”** Wyden said. **“Telehealth**



## Attachment #8

**allows seniors, especially those with multiple chronic conditions, to stay on top of their medical care without taking unnecessary risks or the inconvenience of leaving home. The COVID-19 pandemic has been a trial by fire, but the experience to date has made clear that the health care system is ready for broader access to telehealth on a permanent basis. I'm also proud to say that my bill makes mental health care via telehealth a right for all seniors in Medicare, which is more necessary than ever at a time of increased isolation and anxiety such as this.”**

Earlier this year, Congress took steps to expand access to telehealth in Medicare on a temporary basis during the pandemic. Wyden's bill would permanently eliminate key statutory barriers, making mental health services and commonplace medical visits (known as evaluation and management (E/M) services) available through telehealth to all Medicare beneficiaries and allowing those telehealth services to be provided to beneficiaries in the comfort of their own homes – even after the COVID-19 public health emergency has ended.

The bill goes beyond any steps the Centers for Medicare & Medicaid Services (CMS) can take with its existing authority, by removing the statutory geographic restrictions and expanding the available originating sites for those telehealth services. Under current law, CMS's authority to waive the statutory telehealth requirements in Medicare will lapse when the secretary of Health and Human Services (HHS) declares an end to the public health emergency.

The full legislative language can be found [here](#).



Congresswoman Anna G. Eshoo  
California's 18th Congressional District

## Preeminent Universities and Leading Tech Companies Announce Support for Bipartisan, Bicameral Bill to Develop National AI Research Cloud

June 29, 2020  
Press Release

**Washington, D.C.** – Today, several leading research universities engaged in artificial intelligence (AI) research, technology companies deploying AI technologies, and others announced support for the bipartisan and bicameral *National AI Research Resource Task Force Act*, which establishes a task force to develop a roadmap for a national AI research cloud.

The *National AI Research Resource Task Force Act* was introduced in the House by Representatives Anna G. Eshoo (D-CA), Anthony Gonzalez (R-OH), and Mikie Sherrill (D-NJ) and in the Senate by Senators Rob Portman (R-OH) and Martin Heinrich (D-NM), founding co-chairs of the Senate AI Caucus. The legislation will convene a group of technical experts across academia, government, and industry to develop a detailed plan for how the U.S. can build, deploy, govern, and sustain a national AI research cloud.

“The widespread support for the *National AI Research Resource Task Force Act* from our country’s preeminent research universities and leading technology firms demonstrates how critical the legislation is for our country to retain our global lead in AI research,” **said Eshoo, Gonzalez, Sherrill, and Portman.** “We thank the universities and companies supporting our bill, and we call on Congress to act on this legislation as soon as possible.”

The *National AI Research Resource Task Force Act* is supported by:

- National Security Commission on Artificial Intelligence Chairman Eric Schmidt and Vice Chairman Bob Work
- Stanford University
- The Ohio State University
- Princeton University
- UCLA
- Carnegie Mellon University
- Duke University

- Pennsylvania State University
- University of Pennsylvania
- Johns Hopkins University
- Allen Institute for AI
- OpenAI
- Mozilla
- IEEE-USA
- Google
- Amazon Web Services
- Microsoft
- IBM
- NVIDIA
- Orbital Insight
- Calypso AI

“The *National AI Research Resource Task Force Act* advances a recommendation endorsed by the National Security Commission on Artificial Intelligence in our First Quarter Recommendations to Congress. It is an essential first step towards establishment of a national resource that would accelerate and strengthen AI research across the U.S. by removing the high-cost barrier to entry of compute and data resources. If realized, this infrastructure would democratize AI R&D outside of elite universities and big technology companies and further enable the application of AI approaches across scientific fields and disciplines, unlocking breakthroughs that will drive growth in our economy and strengthen national security,” said **National Security Commission on Artificial Intelligence Chair Dr. Eric Schmidt and Vice Chair Sec. Bob Work**.

“The *National AI Research Resource Task Force Act of 2020* is vital to American innovation,” said **John Etchemendy, Denning Co-Director, Stanford Institute for Human-Centered Artificial Intelligence and Provost Emeritus at Stanford University**. “A National Research Cloud will give academic researchers the tools needed to advance artificial intelligence far into the future. It will also elevate the ability of all colleges and universities to provide the research and teaching needed to maintain our competitiveness in AI. I applaud Congresswoman Eshoo and Senator Portman on taking the first step towards a National Research Cloud through this key piece of legislation.”

“The Ohio State University supports the *National AI Research Resources Task Force Act*,” said **Morley O. Stone, Senior Vice President for Research at The Ohio State University**. “This bill will explore the creation of a shared cloud computing infrastructure for researchers across the country. By bringing together academia, government and the private sector, we can dramatically increase the speed in which the U.S. can innovate in the highly competitive and rapidly evolving areas of artificial intelligence and machine learning.”

“We applaud Senator Portman and Representative Eshoo for defining this crucial opportunity for tapping into the unique strength of America's AI research community. The current and future potential of groundbreaking technological innovation in the US lies in the numerous talented individuals and teams across the country—the National Research Cloud will be critical in

democratizing access to key resources and empowering these researchers to take our AI capabilities to the next level,” said **Dr. Oren Etzioni, CEO, Allen Institute for AI**.

“As artificial intelligence and machine learning become increasingly core to all of our lives, the *National AI Research Resource Task Force Act of 2020* is an important part of ensuring that the internet remains open and accessible to all. The National AI Resource Task Force is crucial in supporting safe, privacy-preserving and reliable artificial intelligence resources to support researchers across the country,” said **Jofish Kaye, Principal Scientist at Mozilla**.

“IEEE-USA supports S. 3890 / H.R. 7096 and applauds Sen. Portman and Cong. Eshoo for taking this much needed first step. The *National AI Research Resource Task Force Act* will focus our R&D resources, ensuring that the United States maintains our global leadership in this critical technology. By constructing a roadmap of research necessary to mature AI-based technology, and by giving experts from government, industry, and academia access to that information, S. 3890 / H.R. 7096 accelerates our AI capabilities far into the future, and enables us to leverage existing technology to advance the fields and disciplines that benefit from high-performance computing capability,” said **James M. Conrad, Ph.D., President, IEEE-USA**.

“United States investments in Research & Development have enabled remarkable innovations, including the microchip, internet, supercomputers, and the Human Genome Project. A National AI Research Resource will help accelerate US progress in artificial intelligence and advanced technologies by providing academic researchers access to the cloud computing resources necessary for experiments at scale. Google recognizes this is an important opportunity for innovation, built on the principles of interoperability and open standards,” said **Jeff Dean, SVP, Google Research**.

“We applaud Senator Portman and Representative Eshoo for helping advance cloud adoption, fostering American innovation, and ensuring U.S. leadership in artificial intelligence. The AWS Cloud increases efficiency while providing unrivaled scalability and services as it delivers powerful utilization of resources. We look forward to working with Senator Portman and Representative Eshoo to ensure the power of the cloud helps accelerate artificial intelligence research and development, and more,” said **David Levy, VP, US Government, Amazon Web Services**.

“IBM applauds Senators Portman and Heinrich and Representatives Eshoo, Sherrill, and Gonzalez for introducing the *National AI Research Resource Task Force Act*. The bill will significantly accelerate America’s leadership in AI by equipping researchers with data sets and computing power to unlock new breakthroughs, and helping train the next generation of data scientists. We strongly support this bill and look forward to advocating for its passage,” said **Dr. Dario Gil, Director of IBM Research**.

“Researchers need access to massively parallel computing resources to develop and advance AI,” said **Ian Buck, Vice President and General Manager of Accelerated Computing at NVIDIA**. “The world’s largest tech companies have invested billions in developing such systems, and we welcome the federal government’s efforts to accelerate important academic research. The *National AI Research Resources Task Force Act* will help give researchers the tools they need to

advance science and industry. I applaud Congresswoman Eshoo, Senator Portman and the bipartisan, bicameral group of co-sponsors for driving this important initiative.”

“As someone who has spent my career dedicated to understanding artificial intelligence, I am proud to lend my support to the *National AI Research Resource Task Force Act of 2020*. I applaud Congresswoman Eshoo and Senator Portman for their leadership on an issue so critical to our nation’s security,” said **Dr. James Crawford, Founder and CEO, Orbital Insight**.

“Calypso AI applauds Representatives Eshoo, Gonzalez and Sherrill, and Senators Portman and Heinrich, for their leadership in sponsoring this transformative legislation to establish a national AI research resource,” said **Neil Serebryany, the CEO of Calypso AI**. “The research infrastructure that will be created by this legislation is critical to our nation’s ability to lead the world in building secure and operational AI.”

July 9, 2020



## **Privacy and Security Round Up**

### **New Federal Privacy Bills Restrict Use of Facial Recognition Technology**

On June 15, 2020, Sen. Sherrod Brown (D-OH) released a discussion draft of a broad privacy bill, the [Data Accountability and Transparency Act of 2020](#). As stated in the [Press Release](#), the bill rejects the approach of most recent privacy bills, which rely primarily on consumer consent to determine permitted uses of personal information. Instead, it places strict limits on the collection, use, and sharing of personal data, including strong civil rights protections. The bill also includes an outright ban on the use of facial recognition technology and data derived from it for any purpose, and establishes a new federal agency focused exclusively on privacy. Shortly thereafter, on June 25, 2020, a group of Senate and House Democratic lawmakers, led by Sen. Ed Markey (D-Mass.), released a much narrower bill, the [Facial Recognition and Biometric Technology Moratorium Act of 2020](#), which would prohibit the use of, or data derived from, a biometric surveillance system, which includes but is not limited to facial recognition software, unless explicitly authorized by an Act of Congress. It would also condition federal grant funding to state and local governments on those governments implementing a similar law or policy. Any data collected in violation of the bill would not be admissible in judicial proceedings.

*Comments: While the two bills are very different in breadth and scope, they both reflect the growing unease about the use and impact of artificial intelligence technology, particularly that using biometric data, as well as a rejection of the consent model as the primary mechanism for regulating permitted uses and disclosures of personal information.*

### **TCPA Developments: Supreme Court Upholds TCPA and FCC Rejects Broadening Exception for Health-Care Calls**

On July 6, 2020, in [Barr v. American Association of Political Consultants](#), the Supreme Court invalidated an exception to the Telephone Consumer Protection Act (TCPA) for government debt collection calls on First Amendment grounds, but held that this did not cause the rest of the TCPA to be invalidated. This decision follows two declaratory orders issued by the Federal Communications Commission (FCC) on the TCPA on June 25, 2020. In the first [Declaratory Order](#), the FCC declined Anthem Inc.'s request to exempt health-care related wireless calls and texts by health plans and providers from the TCPA's prior express consent requirement as long as consumers were allowed to opt-out after the fact. It also rejected Anthem's request that certain non-emergency, but "urgent," health care-related calls and texts be entirely exempt from the TCPA. The FCC noted that while there is no general exemption for health care-related calls, the calls in question could potentially qualify for the limited exemption to the prior express consent requirement adopted in its 2015 Declaratory Regulation and Order. In reaching its decision, the FCC rejected the argument that calls subject to HIPAA should be exempt from the TCPA, pointing out that HIPAA regulates only the contents of communications, and not the methodology for making them. The second [Declaratory Order](#) clarified that as long as a text messaging platform required users to "to actively and affirmatively manually dial each recipient's number and transmit each message one at a time," it was not an auto-dialer, even if capable of sending a large volume of texts.

*Comments: In Barr, the Supreme Court noted that it was not asked to consider the validity of the FCC's regulatory exceptions to the TCPA, including the exception for certain health-related calls. Therefore, these exceptions were not affected by the ruling. While the FCC's Declaratory Order rejecting Anthem's petition is disappointing for health organizations, it does not narrow any existing TCPA exemptions and can perhaps even be read to contemplate that certain exemptions that some thought to be available only to health care providers might also be available to health plans.*

### **Court Determines Cybersecurity Forensic Investigation Report Does Not Qualify as Attorney Work Product**

On May 26, 2020, in [Capital One Consumer Data Security Breach Litigation](#), a U.S. District Court magistrate judge ordered Capital One to provide a copy of a data breach forensic report prepared by a security consulting firm to

plaintiffs in litigation about the breach. The court found that Capital One had not established that the report was protected from disclosure under the attorney work product doctrine and, specifically, that it had failed to show that the report would not have been prepared in “substantially similar form but for the prospect of the litigation.” This was the case even though the report was prepared at the direction of, and delivered to, outside counsel. In reaching its decision, the court noted Capital One’s longstanding relationship and existing retainer agreement with the security consulting firm for the same services, that payment to the firm was classified as a business, rather than legal, expense at the time the report was prepared, and that the report was shared with various regulators, accountants and the internal incident response team for “regulatory and business reasons,” rather than for purposes of the potential litigation.

***Comments:*** *While Capital One is appealing the decision to a district judge, the decision may be seen as a caution that having outside counsel formally engage and receive the report of a security consultant following a data breach may not alone be enough to establish protection under the attorney work product doctrine.*

### **HHS Releases Spring 2020 Unified Regulatory Agenda Containing Several Privacy Items**

On June 30, 2020, as part of the Administration’s Spring 2020 Unified Regulatory Agenda, the Department of Health and Human Services (HHS) listed several privacy items. These include a [proposed rule](#) (slated for issuance in June 2020) to revise the HIPAA Privacy Rule to remove barriers to coordinated care, which follows a December 2018 Request for Information (RFI) on the same topic. It also includes a couple of final rules to revise the regulations governing the confidentiality of substance use disorder (SUD) patient records (known as Part 2 records). The [more significant](#) of these two final rules would finalize an October 2019 proposed rule to remove barriers to coordinated care and allow additional sharing of information among providers and Part 2 programs.

***Comments:*** *The HHS regulatory agenda did not list a proposed rule to amend Part 2 to implement the major changes to the statute governing Part 2 records made by the CARES Act. Under the CARES Act, HHS is required to issue regulations implementing these changes within 12 months, which would be by March 27, 2021. Many health care organizations are eagerly awaiting these regulations, which should make it much less burdensome to share Part 2 records and would bring Part 2 into closer alignment with HIPAA, and were hoping to see them listed in the HHS regulatory agenda.*

### **California Privacy Law Update**

On June 24, 2020, the California Privacy Rights Act (CPRA), a proposed new privacy law that would expand and strengthen the protections in the California Consumer Privacy Act (CCPA), formally qualified for the November 2020 ballot in California. If approved, the CPRA would go into effect on January 1, 2023 and would supersede the CCPA. The CPRA would also immediately extend to January 1, 2023, the CCPA’s current partial exemptions from the CCPA for personal data collected in connection with business-to-business (B2B) transactions and employee/job applicant data. The California Senate has also proposed legislation to extend the two exemptions until January 1, 2022, presumably in case the CPRA ballot initiative does not pass.

***Comments:*** *According to [polling](#) from October 2019, almost 9 out of 10 California voters support the CPRA. In addition, since it already reflects feedback from industry groups, it is not anticipated that the CPRA will face the same opposition from businesses as did the ballot initiative which was ultimately replaced by the CCPA in 2018. In the meantime, enforcement of the CCPA began on July 1, 2020, even as its final regulations have not yet been approved by the California Office of Administrative Law, despite the request by the California Secretary of State for an expedited review by June 30, 2020.*

***Please contact Diane Sacks at [dsacks@sacksllc.com](mailto: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.***



CREDIT RSS JULY 21, 2020 / 2:36 PM / UPDATED 19 HOURS AGO

# Data privacy laws collide with contact tracing efforts; privacy is prevailing

Todd Ehret

10 MIN READ



NEW YORK(Thomson Reuters Regulatory Intelligence) - \*To read more by the Thomson Reuters Regulatory Intelligence team click here: [bit.ly/TR-RegIntel](https://bit.ly/TR-RegIntel)



The startup screen of the Swisscovid contact tracing application of Switzerland, using Bluetooth and a design called Decentralised Privacy-Preserving Proximity Tracing (DP-3T) to ease the lockdown caused by the coronavirus disease (COVID-19) outbreak is seen in this illustration taken June 24, 2020.

Data privacy and personal information protection became top priorities of lawmakers, regulatory bodies, businesses, and individuals in recent years. Now, however, the widespread rollout of “contact-tracing” applications to fight the COVID-19 pandemic could derail decades of progress in privacy laws, experts fear. However, the new laws might have the opposite effect longer-term by raising the overall awareness of data privacy.

As firms prepare for employees to return to offices, senior managers, compliance, and legal departments are grappling with a complex legal landscape. Actions intended to protect employees may also violate various privacy regulations. Furthermore, an overarching question of the efficacy of such new apps in containing the pandemic indicates that data privacy regulations are not about to fall by the wayside.

Below is an overview of the challenges associated with data privacy, of implications for efforts to fight the pandemic, and guidance for legal and compliance professionals.

## THE LEGAL MINEFIELD

When it comes to privacy, the list of laws, rules, and regulations is exhaustive and dates back several decades. Specific to health and employment regulations, the Health Insurance Portability and Accountability Act (HIPAA) [[go-ri.tr.com/9Vn9ZR](https://www.go-ri.tr.com/9Vn9ZR)] requirements and the U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) are the most significant. OSHA has recently published several resources related to the COVID-19 pandemic and workplace-related issues [[www.osha.gov/SLTC/covid-19/](https://www.osha.gov/SLTC/covid-19/)].

The Americans with Disabilities Act (ADA) and state-specific versions of the law generally prohibit employers from disclosing confidential medical information regarding an employee, which includes the employee’s identity [[here](#)].

The Equal Employment Opportunity Commission (EEOC) announced in guidance on April 22 that employers will be allowed to test employees for COVID-19 before entering a worksite without running afoul of the ADA. But the EEOC stated that employers must maintain all information about employee illness as a confidential medical record in compliance with the ADA.

Newer data privacy laws, such as the European Union's General Data Protection Regulation (GDPR) [[go-ri.tr.com/tfHW8e](https://go-ri.tr.com/tfHW8e)], the California Consumer Privacy Act (CCPA) [[oag.ca.gov/privacy/ccpa](https://oag.ca.gov/privacy/ccpa)], and New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) [[go-ri.tr.com/uw9CFq](https://go-ri.tr.com/uw9CFq)] have been at the forefront of priorities for legal and compliance departments at virtually all businesses in the past couple of years.

Despite the absence of an overarching federal data privacy regulation in the U.S., several states besides California have forged ahead, creating a complex patchwork of regulations.

On the heels of that push, several states, with the help of technology giants, Google and Apple, were also quick to roll out technology to track and control the spread of the coronavirus. The apps were described as voluntary and anonymous, based on Bluetooth tracking technology. Critics have voiced concerns that they could set back years of regulatory efforts with a flood of privacy-compromising data.

## STATES AND COUNTRIES HIT PAUSE

Low participation rates, privacy concerns, and technology glitches have plagued the rollout of similar tracing apps around the world.

Among the states that quickly rolled out contact-tracing apps, in South Carolina, privacy concerns halted tracking efforts by its health department. A coronavirus pandemic spending bill adopted by the state forbade public health officials from using contact-tracing apps on cellular devices.

Other states have taken a "wait-and-see" approach as some have struggled with poor

adoption rates and technology glitches.

Norway was an early adopter, when it rolled out its coronavirus contact-tracing app in April. However, in June, the Norwegian Data Protection Authority ordered the Norwegian Institute of Public Health to suspend the app's use and delete all data collected by the technology. The Data Protection Authority said the app presented a disproportionate risk to privacy given low download rates, estimated at less than 15 percent of individuals over the age of 16.

Norway's move came after Lithuania halted its use of a similar app for suspected violations of EU privacy rules.

The conflict between the Norwegian agencies was viewed as a watershed event by many privacy experts and advocates, as privacy prevailed over public health concerns. Additionally, it bolstered the view that contact-tracing apps are ineffective unless public participation rates exceed 50 percent.

When Singapore rolled out a similar initiative called "TraceTogether," [\[here\]](#) only one-fifth of the population agreed to download it, too few to be effective.

## **DATA PRIVACY ATTORNEY WEIGHS IN**

Corporations also have moved cautiously, and are assessing their options and obligations to their employees surrounding workplace safety.

Debates have emerged on mandatory testing (for COVID-19 and antibodies), temperature monitoring, attestations, vaccinations (when available), and contact-tracing for employees. Privacy and employment attorneys agree that the issues raise "very complex" legal questions covering many rules, regulations, and laws.

Cynthia Cole, special counsel in the Palo Alto technology practice at the law firm Baker Botts, said "contact-tracing apps have been portrayed as anonymized, deletable, and non-violating of existing privacy laws. However, the jury is still out on that."

Cole told Regulatory Intelligence there are significant and multi-faceted concerns in moving forward with this technology. “It could lead to bias in its application and involuntary surveillance and questions as to who holds the data remains — the government or a private company — and whether the data and the process itself is auditable. There must also be some system for deleting the data, but it is not clear how that would be enforced,” she said.

Despite the emergency nature of the pandemic, Cole said, “privacy laws such as CCPA and the SHIELD Act still apply.”

“Employers should have a full understanding of what information is being collected, the reason for collecting it, where it’s being stored, who has access to it, and how it will be used,” Cole said.

## **TAKEAWAYS AND SUGGESTIONS**

As companies plan and contemplate reopening offices, there is a long list of well-intentioned considerations to ensure a safe and healthy workplace. Some considerations are simple and raise little concerns from a privacy or legal standpoint. Others are not as clear cut and could open companies to potential litigation and, or violations of regulations or laws.

The lawyers at Baker Botts and many other firms have published recommendations and best practices to consider when reopening offices. Areas for consideration include; the use of health declarations and questionnaires, thermal screening or temperature-taking, and manual and technological contract-tracing.

Several regulators and law enforcement, including the FBI, have reported an increase in cyber attacks amid the pandemic. Therefore, firms should be mindful not to lower any technology requirements or safeguards, particularly about personal privacy.

Employers must be mindful of laws prohibiting discrimination based on race, color, national origin, and other protected classifications. They should administer testing consistently and avoid discriminatory use.

Companies must clarify the purpose for collecting data from those being tested and tailor the collection to that purpose.

There should be strict prohibitions on the use of any personal data gathered for any other purpose than COVID-19-related health and safety purposes. The data collected should be carefully protected with a plan of disposal when it is no longer needed to fight the pandemic.

Contact-tracing of employees should not be obligatory. Any use of third-party tracing apps should be voluntarily, with the risks adequately disclosed. Many apps have not been entirely vetted for compliance with applicable privacy laws. According to Baker Botts, liability and exposure in the agreements to use third-party apps are extremely important as many contain virtually no protection for the end-user or the company.

Other data privacy concerns include transparency about the purpose of collecting information, the retention period, safeguarding the data, restricting access to the data, and employing anonymization techniques.

Returning to work in a safe office will require planning on the part of many parts of an organization. However, contract-tracing is only one of many options. It is perhaps one of the least effective, with the highest potential for data privacy liability as well.

Skeptics that thought data privacy might be shunned or set back as a result of the public health crisis are thus far being proven wrong. The heightened awareness and caution surrounding data privacy indicate that the regulations are here to stay, and new data privacy laws will likely gain momentum in the future.

(Todd Ehret, Regulatory Intelligence. Julie DMAuro of Regulatory Intelligence contributed to this article)

This article was produced by Thomson Reuters Regulatory Intelligence - [bit.ly/TR-RegIntel](https://bit.ly/TR-RegIntel) - and initially posted on July 13. Regulatory Intelligence provides a single source for regulatory news, analysis, rules and developments, with global coverage of more than 400 regulators and exchanges. Follow Regulatory Intelligence compliance news on Twitter: @thomsonreuters

*Our Standards: [The Thomson Reuters Trust Principles](#).*



June 16, 2020

**PRESIDENT**  
**Tim Fox**  
*Montana Attorney General*

Mr. Sundar Pichai  
Chief Executive Officer  
Google, LLC  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Mr. Tim Cook  
Chief Executive Officer  
Apple, Inc.  
1 Apple Park Way  
Cupertino, CA 95014

**PRESIDENT-ELECT**  
**Karl A. Racine**  
*District of Columbia  
Attorney General*

**VICE PRESIDENT**  
**Tom Miller**  
*Iowa Attorney General*

**IMMEDIATE PAST PRESIDENT**  
**Jeff Landry**  
*Louisiana Attorney General*

**EXECUTIVE DIRECTOR**  
**Chris Toth**

Dear Mr. Pichai and Mr. Cook:

The undersigned Attorneys General (“State Attorneys General”) write to express our strong concerns regarding the proliferation of contact tracing apps on your platforms that do not sufficiently protect consumers’ personal information. Digital contact tracing may provide a valuable tool to understand the spread of COVID-19 and assist the public health response to the pandemic. However, such technology also poses a risk to consumers’ personally identifiable information, including sensitive health information, that could continue long after the present public health emergency ends.

We are aware of your companies’ joint development of application programming interfaces (APIs) that may be used to build decentralized exposure notification and contact tracing apps that utilize Bluetooth. Additionally, we understand from press reports and online materials that those APIs will only be available to public health authorities and that use of the APIs will be contingent on the inclusion of certain features to protect consumer privacy.

While we welcome your stated focus on a privacy-centered notification and tracing tool for future use, several COVID-19 related contact tracing apps are already available on Google Play and the App Store. Some of those apps may endanger consumers’ personal information. We are particularly concerned about purportedly “free” apps that utilize GPS tracking, contain advertisements and/or in-app purchases, and are not affiliated with any public health authority or legitimate research institution.<sup>1</sup>

Moreover, as public health authorities release apps built with your APIs, there is likely to be increased media and consumer attention on exposure notification and contact tracing apps. Other developers may take advantage of the situation by placing new contact tracing apps on your platforms that do not adequately safeguard consumers’ personal information

1850 M Street, NW  
Twelfth Floor  
Washington, DC 20036  
Phone: (202) 326-6000  
<https://www.naag.org/>

<sup>1</sup> For instance, as recently as early May, the first result when a consumer searches “contract tracing” on both platforms was an app called “Contact Tracing” developed by Piusworks, LLC, a California company with a suspended registration. According to the app information previously disclosed on Google Play, Contact Tracing uses geolocation tracking, contains ads, and offers in-app purchase, and it has been installed over 50,000 times. The app has since been removed from Google Play but is still available on the App Store.

in compliance with our states' laws. Therefore, we urge Google and Apple to take the following actions with respect to exposure notification and contact tracing apps available to U.S. consumers on Google Play and the App Store:

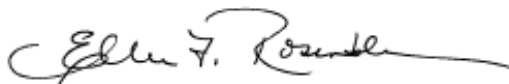
1. Verify that every app labeled or marketed as related to contact tracing, COVID-19 contact tracing, or coronavirus contact tracing or exposure notification is affiliated with a municipal, county, state or federal public health authority, or a hospital or university in the U.S. that is working with such public health authorities;
2. Remove any app that cannot be verified consistent with the above; and
3. Pledge to remove all COVID-19 / coronavirus related exposure notification and contact tracing apps, including those that utilize your new APIs, from Google Play and the App Store once the COVID-19 national emergency ends.<sup>2</sup> In addition, provide written confirmation to our offices that the apps have been removed or an explanation why removal of a particular app or apps would impair the public health authorities affiliated with each app.

Implementing these limited measures could help protect the personally identifiable information and sensitive health data of millions of consumers during this crisis.

Sincerely,



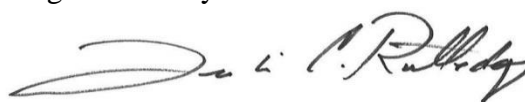
Douglas Peterson  
Nebraska Attorney General



Ellen F. Rosenblum  
Oregon Attorney General



Kevin G. Clarkson  
Alaska Attorney General



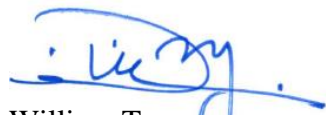
Leslie Rutledge  
Arkansas Attorney General



Xavier Becerra  
California Attorney General



Phil Weiser  
Colorado Attorney General



William Tong  
Connecticut Attorney General

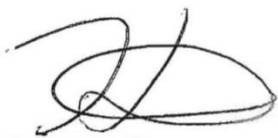


Kathleen Jennings  
Delaware Attorney General

---

<sup>2</sup> This refers to the expiration of the emergency declared by the Secretary of Health and Human Services on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. 247d), and any renewals thereof.





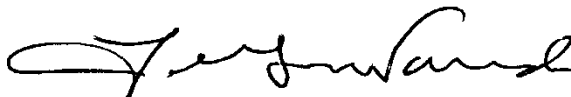
Karl A. Racine  
District of Columbia Attorney General



Leevin Taitano Camacho  
Guam Attorney General



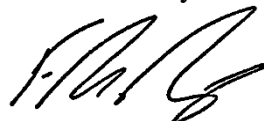
Clare E. Connors  
Hawaii Attorney General



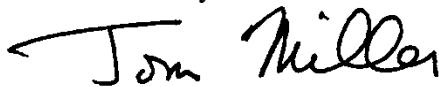
Lawrence Wasden  
Idaho Attorney General



Kwame Raoul  
Illinois Attorney General



F. Aaron Negangard  
Indiana Chief Deputy Attorney General



Tom Miller  
Iowa Attorney General



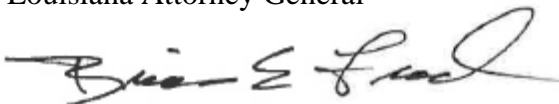
Derek Schmidt  
Kansas Attorney General



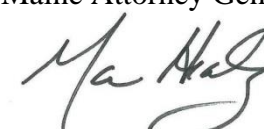
Jeff Landry  
Louisiana Attorney General



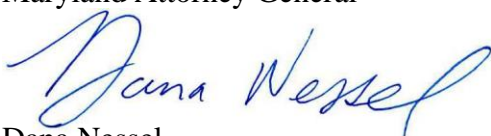
Aaron M. Frey  
Maine Attorney General



Brian Frosh  
Maryland Attorney General



Maura Healey  
Massachusetts Attorney General



Dana Nessel  
Michigan Attorney General



Keith Ellison  
Minnesota Attorney General



Aaron D. Ford  
Nevada Attorney General



Gordon MacDonald  
New Hampshire Attorney General



Gurbir S. Grewal  
New Jersey Attorney General



Hector Balderas  
New Mexico Attorney General





Josh Stein  
North Carolina Attorney General



Wayne Stenehjem  
North Dakota Attorney General



Dave Yost  
Ohio Attorney General



Mike Hunter  
Oklahoma Attorney General



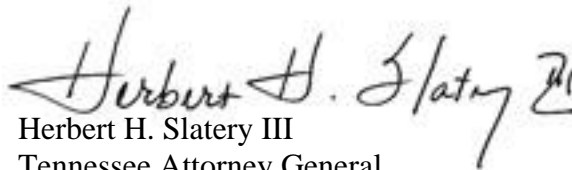
Josh Shapiro  
Pennsylvania Attorney General



Dennise N. Longo Quiñones  
Puerto Rico Attorney General



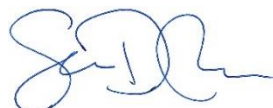
Peter F. Neronha  
Rhode Island Attorney General



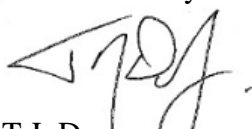
Herbert H. Slatery III  
Tennessee Attorney General



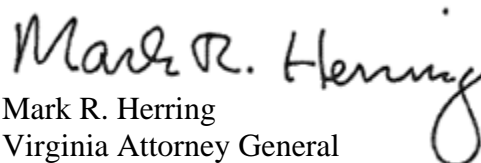
Ken Paxton  
Texas Attorney General



Sean Reyes  
Utah Attorney General



T.J. Donovan  
Vermont Attorney General



Mark R. Herring  
Virginia Attorney General



Patrick Morrissey  
West Virginia Attorney General

## Personal privacy – Does the pandemic change the rules?

The pandemic has inevitably made discussions about the use of data even more urgent as we strive to find solutions to dilemmas around managing personal privacy argues Dr Charles Alessi, chief clinical officer at HIMSS.

By [Charles Alessi](#)

July 13, 2020

05:24 AM



It is helpful to explore this dilemma a little bit further. Rules and legislation around the right to personal privacy is at the heart of our standing and relationships within communities. Given the extent to which the use of devices is now ubiquitous, as well as the potential for data associated with these devices to identify individuals and when aggregated with other data, to provide a fuller picture of an individual's habits, the fact that there is strict legislation controlling this is a positive factor.

In different jurisdictions, there are different rules that manage these data flows. In the US it's Health Insurance Portability and Accountability Act (HIPAA), in the European Union it's the General Protection Data Regulation (GDPR) that regulates the use of data and this is mirrored to a greater or lesser extent in most of the other countries in the world. While the interpretation of data legislation is often a contentious issue, and in places there are instances where it impeded, not assisted data transfer, the mainstream judgement is that these rules are worthy as they protect us, the citizens, from the indiscriminate use of our data by everyone from major corporations to governments.

The pandemic does introduce another dimension into this discussion, however. It is widely acknowledged that for effective management of outbreaks, it is necessary to identify, then track and trace every individual who is potentially at risk of developing COVID-19, specifically when individuals could well be shedding virus and be infective prior to the development of symptoms. In looking around the world at which countries have been particularly successful at managing the first wave of COVID-19, they tend to be ones which instituted processes around test, track and trace early and comprehensively. To do this with the requisite speed and scale, it is beneficial to use electronic means to contact trace, as happened in Taiwan, South Korea, Singapore and a host of other countries.

The implication is that people's right to personal privacy around data is then secondary to the right of citizens to be protected from a contagion. These dilemmas are not new in medicine. Patient confidentiality is sacrosanct in medical practice unless there is a duty to protect others that could be harmed. There is even a process to notify authorities of diseases which have the propensity to infect populations quickly, like typhoid and conditions such as yellow fever.

There are some sound principles, however, that could be deployed to try to ensure as much confidentiality and privacy as possible to the citizen, while satisfying the need for public health systems to perform the functions they need to implement, to limit the spread of contagious disease. These include:

## **1. Safeguarding privacy**

There are various initiatives available today which make it possible to preserve privacy and ensure there is no potential for data to be misused. The most topical one is the Apple, Google initiative. This is a process where data is never centralised, lives on your phone, is automatically erased and cannot thus be misused, even being inaccessible to others by court order. This initiative has now become the basis for a whole group of countries within the European Union and beyond and it's an unusual example of major corporations working together for the common good. It is still unclear whether the applications produced will afford the citizens enough confidence that large enough numbers will download them and make the apps useful.

## **2. Sunset clauses**

Unless one is using the decentralised methods described above, it is helpful to have enacted a "sunset clause" in legislation to ensure personal data will no longer be available once the emergency of the pandemic is over.

## **3. Secondary use of data legislation**

This is always a contentious subject but there are examples of countries that have found solutions to utilise aggregated databases. FinData, the Health and Social Data permit Authority in Finland is noteworthy in this regard as an example of transparency and excellent practice. Set up in 2019, it regulates the use of data stored by various other national controllers including private controllers and stored in Kanta services (as of 2021).

## **4. Foresight**

South Korea has much to teach us here. Following the MERS coronavirus outbreak in 2015, legislation was implemented only to be used in a pandemic emergency, then rescinded. This legislation really changed the existing strict data guardianship rules when implemented as it allowed for an extremely comprehensive strategy for contact tracing, whereby anyone who has interacted with an infected person is traced and quarantined. This included allowing access from credit card companies, and location from cell phone carriers. This was implemented as soon as the pandemic reached South Korea, and together with other robust measures successfully protected the population from the first wave.

## **5. Establishing trust**

This is the most valuable of all the principles and the most difficult to maintain. Populations tend to be compliant with requests from governments if significant trust exists between the citizen and the government. This is supported by a well-developed communication strategy underpinned by the use of transparency in the way data is presented.

The balance of views suggests that we are likely to see a second wave and it is essential we prepare for the second wave to ensure we manage to shield our populations better. These debates around privacy and the duty of each citizen not to harm others through contagion should be taking place now if they have not taken place previously, as this will enable us to be in the optimal place when and if the second wave strikes. We must use this time wisely.

**A Technical Approach to Shore up FTC Consumer Protections for  
Electronic Health Record-Connected Apps**

**Raheel Sayeed, James Jones, Daniel Gottlieb, Joshua C. Mandel, Kenneth D. Mandl**

**Computational Health Informatics Program,**

**Boston Children's Hospital, Boston, MA**

A patient can, under the Health Insurance Portability and Accountability Act (HIPAA), request a copy of her medical records in a “form and format” of her choice “if it is readily producible.” However, patient advocates have long complained about a process which is onerous, inefficient, at times expensive, and almost always on paper. The patient-driven healthcare movement [1] advocates for turnkey electronic provisioning of medical record data to improve care and accelerate cures.

There is recent progress. The 21st Century Cures Act [2] requires that certified health information technology provide access to all data elements of a patient's record, via published digital connection points, known as application programming interfaces (APIs), that enable healthcare information “to be accessed, exchanged, and used without special effort.” In March, the Secretary of Health and Human Services announced a new rule, from The Office of the National Coordinator of Health Information Technology (ONC), facilitating a standard way for any patient to connect an app of her choice to her provider's electronic health record (EHR). With these easily added or deleted (“substitutable” apps [3]), she should be able to obtain a copy of her data, share it with health care providers and apps that help her make decisions and navigate her care journeys, or contribute data to research. Because the rule mandates the “SMART on FHIR” API [4] (an open standard for launching apps [5] that we developed, now part of Health Level Seven's Fast Healthcare Interoperability Resources [6] ANSI Standard), these apps will run anywhere in the health system.

Apple recently advanced an apps-based information economy [7], by connecting its native “Health app” via the SMART on FHIR API, to hundreds of health systems [8], so patients can download copies of their data to their iPhones. The rule will no doubt spark the development of a substantial number of additional apps.

Policymakers are grappling with concerns that data crossing the API and leaving a HIPAA covered entity [9] are no longer governed by HIPAA. Instead, commercial apps and the data therein fall under oversight of the Federal Trade Commission (FTC) under Section 5(a) of the FTC Act (FTCA) which prohibits “unfair or deceptive acts or practices in or affecting commerce [10].”

When a patient obtains her data via an app, she will likely have agreed to the terms of service or at least clicked through an agreement [11] no matter how lengthy or opaque the language. She should also have access to the privacy policy. For commercial apps in particular, these are often poorly protective [12]. As with consumer behavior in the non-healthcare apps and services

marketplace, we expect that many patients will broadly share their data with apps, unwittingly giving up control over the uses of those data by third parties [13]. FTC does not regulate the content of terms or privacy policies.

Because ONC's regulatory authority over EHR does not extend to regulating consumer health apps, the new rule which promotes interoperability begs for concomitant protections for patients, who will naturally be drawn to use apps that help them manage their care and contribute to public health and research. Some patients may wish to explore the nascent emerging marketplace offering options to monetize their data. "Information altruists" [14] and self-assembling patient groups will donate data [15] to speed social and direct benefit through innovation and research. (Notably, the monetary value of an individual record is generally low, with exceptions for patients having rare or complex conditions and histories).

How do we support a patient's autonomy to use tools of her choice to improve her health and contribute to research, provide her with options to share in the monetary value from downstream uses of her data, while also protecting her from predatory practices?

HIPAA does not adequately address the issue. While it does allow an app developer to become a business associate [9] of a covered entity (such as a provider or healthcare institution) this arrangement only applies when an app is managing health information on behalf of the covered entity — whereas in a consumer-centric ecosystem, many apps will choose to have a relationship with a consumer directly. Importantly, the covered entity itself may be a conflicted party when the patient wishes to use an app that either (1) shares data with a competing health care provider or (2) competes with the functionality of the entity's EHR. These conflicts could limit data flow across institutions, and raise the barrier to entry for new, innovative apps.

Further, the HIPAA business associate framework *does not* prevent commercial use of patient's data without consent. Patient data in de-identified format are already shared widely in healthcare on hundreds of millions of patients, generally in ways that are opaque and not reported to the patients whose data have oftentimes been aggregated, sold, and used for profit, and sometimes in ways that enable downstream re-identification [16].

A federal task force recognized that enabling patient autonomy to share data comes with inherent risk, and largely left these trade-offs in the patient's hands [17]. There are promising approaches available to protect a patient's health data without limiting choice or creating a bottleneck to innovation by new and smaller entrants into the Health IT ecosystem. Now is the time to consider these carefully. Ultimately, solutions will likely include a mix of legislation, regulation, and best practices. Here, we focus on strengthening the FTC's capacity to protect patients, exploring two pathways.

## **Methods**

Our first approach is to standardize the terms of service and privacy policies presented to consumers when interacting with EHR-connected apps:

The extended federal responses to comments on the ONC rule [18] require that privacy notices for apps accessing a patient's electronic health information (EHI) must be at a minimum (1)

made publicly accessible at all times, including updated versions; (2) shared with all individuals that use the technology prior to the technology's receipt of EHI from an actor; (3) written in plain language and in a manner calculated to inform the individual who uses the technology; (4) include a statement of whether and how the individual's EHI may be accessed, exchanged, or used by any other person or other entity, including whether the individual's EHI may be sold at any time (including in the future); and (5) include a requirement for express consent from the individual before the individual's EHI is accessed, exchanged, or used, including receiving the individual's express consent before the individual's EHI is sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction).

In the interest of allowing information to flow freely, the commentary further suggests [19] that patient-facing privacy notices should be focused on any current privacy and/or security risks posed by the technology or the third-party developer of the technology. They are also encouraged to be provided in a non-discriminatory manner, factually accurate, unbiased, objective, and not unfair or deceptive.

To consider the realizability of these requirements, we analyzed privacy risks touched on by the ONC's 2018 Model Privacy Notice,[20] elements in sample questionnaires that EHR vendors are already leveraging during security and privacy reviews of third-party applications, and items addressed in codes of conduct such as the CARIN Code of Conduct [21]. We note here that leveraging an ecosystem of codes of conduct may be a complementary approach to any text in a privacy notice to a patient, as many current privacy practices are difficult to capture succinctly.

**Table 1** summarizes observed overlaps in approaches to address common data privacy concerns consumers face when moving health data from a covered entity to a consumer app.

<b>Data Privacy Concern:</b>	<b>Listed in 2018 Model Privacy Notice</b>	<b>Observed in EHR app developer questionnaire</b>	<b>Addressed in CARIN Code of Conduct</b>
Is all or some of the data you collect covered under HIPAA?	Y	Y	Y
How is identifiable data used internally?	Y	Y	Y
How is identifiable data shared?	Y	Y	Y
How is de-identified data shared or sold?	Y	Y	Y
Where is de-identified data sold?	Y	Y	Y
Where is identifiable data stored?	Y	Y	Y
When is data encrypted?	Y		Y
Is the user allowed to (access/edit/share/delete) their data?	Y	Y	Y

What happens to your data when your account is deactivated?	Y	Y	Y
How are users notified in the case of an improper disclosure?	Y		Y
What potential impact does sharing this data have on others including your family?			Y
Is this a one time collection of data or authorization for future access?			Y
Are user changes to data able to be viewed when that data is shared with other parties?			Y
What happens to user data under transfer of ownership by the developer?			Y

Table 1. Approaches to identifying current privacy risks.

The SMART on FHIR specification [5] is standardized in the ONC rule as a universal connector between third-party applications and an EHR. SMART includes a health-specific implementation of the widely adopted open standard OAuth that allows apps to gain authorized access without the user having to disclose their credentials to the third-party app-developer. As the app initiates the OAuth authorization routine (“App Authorization”), the user is explicitly redirected to an authorization interface by the EHR to seek approval for allowing the app access to her data. This interface clearly identifies the app making the request along with the data (scopes) the app is seeking from the EHR. This technical underpinning of the app authorization process provides an opportunity for a dialogue with the patient.

### Results

Within the SMART on FHIR specification, we have identified opportunities (1) to create a standardized *privacy manifest* with a minimal set of variables and text that attempts to distill an app-developer’s privacy policy for all actors (including the EHR vendors, health systems and end users); (2) for app developers to declare this privacy manifest and have it shared with the EHR at the time of the app registration and (3) for EHRs to relay and present the manifest in a non-discriminatory manner to the patients for access approval.

*Privacy Manifest Categories.* Communicating the Privacy Manifest is technically accomplishable as part of the SMART specification within its “App Authorization sequence (described above) that is also referenced in the ONC rules– in a response to the privacy policies of third party patient-facing apps that are not subject to HIPAA [18]. Box 1 shows identified data artifacts which can be reported by the app developer and communicated during the SMART workflow with minimal effort. Care must be taken to ensure the items rendered to the patient are accurate and broadly interpretable and understandable across literacy levels and diverse backgrounds, including different native languages.



Artifact able to be captured from app developers and then displayed to the patient during SMART on FHIR authorization	Description
Privacy policy URL	Location of the full privacy policy for review
Data Storage policy	Information about how patient data is stored
Data Usage policy	Who can get access to full, de-identified, or aggregate patient data and what is the intent of its use?
Data Sharing policy	Who may the app developer send the data to and for what purpose?
Data Selling policy	What relevant data, if any, from the patient may be sold by the app developer?
Consent before sharing	The app's method for approaching patients before sharing their data with other parties
Trust Entities (badges)	Icons and links to any relevant trust entities claimed by the app developer

*App registration with the EHR.* Apps require a client identifier from the EHR along with its endpoints for data access. This is obtained after registration of the app. EHRs may capture the privacy manifest as part of this existing registration process by presenting a survey and capturing granular “yes or no” responses to specific privacy questions along with the regular elements that are part of the SMART specification

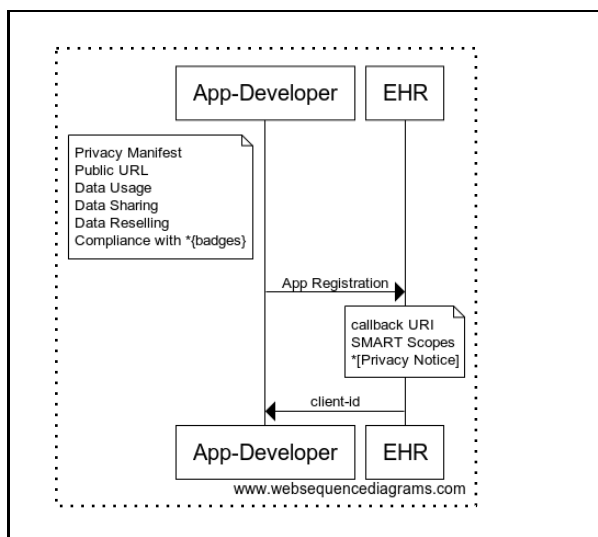


Figure 1. App registration with the EHR. The EHR performs a privacy and security evaluation with the app developer prior to registration and populates the app's SMART Scopes and privacy manifest then shares the client-id with the App

developer.

*Presenting Manifest to the User.* When the end-user launches the app, the app seeks

authorization to access the EHR, at which point the EHR evaluates the request and presents an app authorization interface in the form of a web page to the user seeking her approval for allowing app access to the data. It is at this juncture, that the “privacy manifest” is populated into the authorization web page with the appropriate level of “caution” or “warning” indication informing the user of the privacy policies pertaining to each of the categories of the manifest—*“storage, usage, sharing, selling, consent for share”* and a url link out to the privacy policy of the app. From here on, the user has two choices: either approve the app’s access to her data in the EHR or deny.

### Discussion

Transparency in apps’ sharing policies with regards to research use and monetization can empower patients to decide to share more data with good actors and avoid those apps unwilling to meaningfully disclose their practices. We view leveraging the OAuth dialogue for communicating privacy manifests as a potentially critical intermediate step to inform patients of the implications of moving their health data into consumer apps, pending more robust privacy protections or strengthening of FTC enforceability. These manifests can serve all modalities of a third-party app (web or device native) and can additionally be absorbed by smartphone app stores to be rendered to the user upon installation of the app.

Further consultation with stakeholder experts is needed to iterate upon a common, standardizable manifest with granular questions able to extract key elements of a patient health privacy policy. Of note, EHR vendors or providers are able to require updates to the manifest from app developers as needed, reaffirming privacy policies on emergent issues to patients.

### References

1. Mandl KD, Kohane IS. Time for a Patient-Driven Health Information Economy? *N Engl J Med.* Jan 21 2016;374(3):205-208.
2. 114th Congress. H.R.34 - 21st Century Cures Act; 2015-2016.
3. Mandl KD, Kohane IS. No small change for the health information economy. *N Engl J Med.* Mar 26 2009;360(13):1278-1281.
4. Computational Health Informatics Program. SMART Health IT. <http://smarthealthit.org>.
5. HL7, Computational Health Informatics Program BCsH. SMART Application Launch Framework Implementation Guide Release 1.0.0. <http://www.hl7.org/fhir/smart-app-launch/>.
6. HL7. HL7 FHIR Foundation. <http://www.fhir.org/>.
7. Mandl KD, Mandel JC, Kohane IS. Driving Innovation in Health Systems through an Apps-Based Information Economy. *Cell Syst.* Jul 2015;1(1):8-13.
8. Mandl KD. Apple will finally replace the fax machine in health care. *CNBC* <https://www.cnn.com/2018/01/30/apple-will-finally-replace-the-fax-machine-in-health-care-commentary.html>; 2018.
9. Services DoHaH. Covered Entities and Business Associates. *HHS*. [\[https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html\]](https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html).
10. . Title 15 U. S. Code §45.

11. Cakebread C. You're not alone, no one reads terms of service agreements. *Business Insider* [<https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=UK>].
12. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. *J Am Med Inform Assoc*. Apr 2015;22(e1):e28-33.
13. Mandl KD, Kohane IS. Data Citizenship under the 21st Century Cures Act. *N Engl J Med*. Mar 11 2020.
14. Kohane IS, Altman RB. Health-information altruists--a potentially critical resource. *N Engl J Med*. Nov 10 2005;353(19):2074-2077.
15. Taylor PL, Mandl KD. Leaping the Data Chasm: Structuring Donation of Clinical Data for Healthcare Innovation and Modeling. *Harvard Health Policy Rev*. Spring 2015;14(2):18-21.
16. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun*. Jul 23 2019;10(1):3069.
17. Committee HIPaS. API Task Force Recommendations. [https://www.healthit.gov/sites/default/files/facas/HITJC\\_API TF\\_Recommendations.pdf](https://www.healthit.gov/sites/default/files/facas/HITJC_API TF_Recommendations.pdf).
18. Office of the National Coordinator of Health Information Technology. 21st Century Cures Act: Interoperability Information Blocking and the ONC Health IT Certification Program. *45 CFR Parts 170 and 171 RIN 0955-AA01*. Page 678; 2020.
19. Office of the National Coordinator of Health Information Technology. 21st Century Cures Act: Interoperability Information Blocking and the ONC Health IT Certification Program. *45 CFR Parts 170 and 171 RIN 0955-AA01*. Page 675; 2020.
20. Office of the National Coordinator of Health Information Technology. The Model Privacy Notice (MPN) <https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf>.
21. CARIN Alliance. CARIN Code of Conduct. [https://www.carinalliance.com/wp-content/uploads/2019/05/2019\\_CARIN\\_Code\\_of\\_Conduct\\_05082019.pdf](https://www.carinalliance.com/wp-content/uploads/2019/05/2019_CARIN_Code_of_Conduct_05082019.pdf).