



Confidentiality Coalition General Committee  
Thursday, February 18  
3:00PM – 4:00PM EST

Zoom Link: <https://zoom.us/j/93839752716?pwd=RE9jSWh5a3U4UngyMXVEbDBwSmp6dz09>  
Meeting ID: 938 3975 2716  
Phone Number: 301-715-8592  
Password: 253132

1. Welcome and Introductions
2. Guest Speaker-2021 Congressional Privacy Landscape  
Amy Tejral, Partner, Avenue Solutions Attachment 1
3. HIPAA Coordinated Care Rule
4. TCPA Update Attachment 2
5. Biden Data Sharing Executive Order Attachment 3
6. HHS Artificial Intelligence Strategy Attachment 4
7. Information Blocking Final Rule Implementation Date
8. CDT/eHI Consumer Privacy Framework for Health Data Attachment 5
9. Privacy Round-Up Attachment 6
10. Articles of Interest Attachment 7, 8, 9, 10

Privacy Bills 117<sup>th</sup> Congress

Bill Number	Title	Introduced	Sponsor	Committee
H.R. 847	To support research on privacy enhancing technologies and promote responsible data use, and for other purposes	2/4/21	Stevens (D-MI)	Science
S. 224	A bill to support research on privacy enhancing technologies and promote responsible data use, and for other purposes	2/4/21	Cortez Masto (D-NV)	Science

Privacy Bills 117<sup>th</sup> Congress

H.R. 651	Public Health Emergency Privacy Act	2/1/21	Eshoo (D-CA), Schakowsky (D-IL), DelBene (D-WA), Beyer (D-VA), McNerney (D-CA), Barragan (D-CA), Pocan (D-WA), Rush (D-IL), Welch (D-VT), Scanlon (D-PA), Matsu (D-CA), Lieu (D-CA), DeSaulnier (D-CA), Hayes (D-CT), Khanna (D-CA), Garcia (D-IL), Lynch (D-MA), Grijalva (D-AZ), Lee (D-CA), Dingell (D-MI), DeFazio (D-OR), Johnson (D-GA), Porter (D-CA), Davis (D-IL), Carson (D-IN)	E&C
----------	-------------------------------------	--------	---	-----

Privacy Bills 117<sup>th</sup> Congress

S. 113	A bill to require providers of broadband internet access service and edge services to clearly and conspicuously notify users of the privacy policies of those providers, to give users opt-in or opt-out approval rights with respect to the use of, disclosure of, and access to user information collected by those providers based on the level of sensitivity of the information, and for other purposes	1/28/21	Blackburn (R-TN)	Commerce
--------	--	---------	------------------	----------

Privacy Bills 117<sup>th</sup> Congress

S. 81	Public Health Emergency Privacy Act	1/28/21	Blumenthal (D-CT), Warner (D-VA), Markey (D-MA), Baldwin (D-WI), Hirono (D-HI), Booker (D-NJ), Menendez (D-NJ), King (I-ME), Bennet (D-CO), Warren (D-MA), Klobuchar (D-MN), Durbin (D-IL)	HELP
-------	-------------------------------------	---------	--	------

Privacy Bills 117<sup>th</sup> Congress

S. 24	Protecting Personal Health Data Act	1/22/21	Klobuchar (D-MN), Murkowski (R-AK), Cortez Masto (D-NV)	HELP
-------	-------------------------------------	---------	---	------

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

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

**DECLARATORY RULING**

**Adopted: January 15, 2021**

**Released: January 15, 2021**

By the Chief, Consumer and Governmental Affairs Bureau:

**I. INTRODUCTION**

1. The Telephone Consumer Protection Act (TCPA) and the Commission’s implementing rules generally prohibit a caller from making an artificial or prerecorded voice message call to any residential telephone line without the consumer’s prior express consent.<sup>1</sup> The Commission’s rules, however, exempt from the prior-express-consent requirement prerecorded calls that are not made for a commercial purpose and those made for a commercial purpose but that do not include or introduce an advertisement or constitute telemarketing.<sup>2</sup> The Commission recently limited these exemptions to three calls within any consecutive 30-day period and required callers to allow consumers to opt out of future calls.<sup>3</sup>

2. Acurian, Inc. filed a petition for declaratory ruling asking the Commission to clarify that a call to a residential telephone line seeking an individual’s participation in a clinical pharmaceutical trial is not subject to the TCPA’s restrictions on prerecorded calls.<sup>4</sup> Acurian argues that its calls are not made for a commercial purpose or, alternatively, do not include or introduce an advertisement or constitute telemarketing, and thus do not require the individual’s prior express written consent.<sup>5</sup>

3. In this declaratory ruling, we apply the Commission’s existing rules and precedent and clarify that an artificial or prerecorded voice message call to a residential telephone line seeking a consumer’s participation in a clinical pharmaceutical trial but not including any advertising or telemarketing is exempt from the TCPA’s prior-express-written-consent requirement as long as the caller

---

<sup>1</sup> See 47 U.S.C. §§ 227(b)(1)(B), (b)(2)(B); 47 CFR § 64.1200(a)(3) (requiring that the prior express consent be written).

<sup>2</sup> See 47 CFR §§ 64.1200(a)(3)(ii), (iii). The rules also exempt calls made for an emergency purpose; calls made by or on behalf of a tax-exempt nonprofit organization; and calls that deliver a “health care” message made by, or on behalf of, a “covered entity” or its “business associate,” as those terms are defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. See *id.* §§ 64.1200(a)(3)(i), (iv), (v).

<sup>3</sup> See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, FCC 20-186, at paras. 15, 21, and 28-29 (Dec. 30, 2020) (*2020 TCPA Exemptions Order*).

<sup>4</sup> See Acurian, Inc., Petition for Declaratory Ruling Regarding Telephone Communications Seeking Candidates for Clinical Trials, CG Docket No. 02-278 (filed Feb. 5, 2014) (Petition).

<sup>5</sup> *Id.*

makes no more than three such calls within any consecutive 30-day period and allows the called party to opt out of future calls. We thus grant Acurian's Petition.

## II. BACKGROUND

4. In relevant part, the TCPA makes it unlawful to “initiate any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party, unless the call is initiated for emergency purposes . . . or is exempted by rule or order by the Commission . . . .”<sup>6</sup> The TCPA authorizes the Commission, “by rule or order,” to exempt “(i) calls that are not made for a commercial purpose; and (ii) such classes or categories of calls made for commercial purposes as the Commission determines—(I) will not adversely affect the privacy rights that this section is intended to protect; and (II) do not include the transmission of any unsolicited advertisement.”<sup>7</sup>

5. Implementing this statutory authority, the Commission has exempted from the prohibition any artificial or prerecorded voice call that is “not made for a commercial purpose” or “made for a commercial purpose but does not include or introduce an advertisement or constitute telemarketing,” amongst other exemptions.<sup>8</sup> Over the years, the Commission has applied its rules in a variety of specific contexts.<sup>9</sup> And, very recently, the Commission limited these exemptions to three calls within any consecutive 30-day period and required callers to allow consumers to opt out of future calls.<sup>10</sup>

---

<sup>6</sup> 47 U.S.C. § 227(b)(1)(B).

<sup>7</sup> *Id.* § 227(b)(2)(B).

<sup>8</sup> 47 CFR §§ 64.1200(a)(3)(ii), (iii).

<sup>9</sup> *See, e.g., Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14097-98, paras. 140-42 (2003) (*2003 TCPA Order*) (determining that an autodialed or prerecorded call that consists of a free offer, coupled with offers of goods or services for sale, either during or after the call, constitutes an advertisement and is prohibited, unless otherwise exempted); *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Second Order On Reconsideration, 20 FCC Rcd 3788, 3803-04, paras. 38-39 (2005) (*2005 TCPA Order*) (finding that calls by real estate agents who represent only the potential buyer to someone who has advertised their property for sale do not constitute telephone solicitations, so long as the purpose of the call is to discuss a potential sale of the property to the represented buyer, as such callers are not encouraging the called party to purchase, rent or invest in property, as contemplated by the definition of “telephone solicitation”); *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 27 FCC Rcd 1830, 1838-40, paras. 20-26 (2012) (*2012 TCPA Order*) (revising the rules to require prior express written consent for all autodialed and prerecorded telemarketing calls to wireless numbers and residential lines).

<sup>10</sup> *See 2020 TCPA Exemptions Order*, at paras. 15, 21, and 28-29. The exemption for HIPAA-related calls has a different limitation of one call per day, up to three calls per week. *Id.* at para. 38.



6. In 2014, Acurian filed a petition for declaratory ruling asking the Commission to clarify that a telephone call to a residential telephone line seeking an individual's participation in a clinical pharmaceutical trial is exempt from the TCPA's restrictions on prerecorded calls.<sup>11</sup> Acurian describes itself as "a leading full-service provider of clinical trial patient recruitment and retention solutions for the life sciences industry" that identifies potential candidates for particular clinical pharmaceutical trials—often using prerecorded voice messages to provide introductory information with the opportunity for a live follow-up call.<sup>12</sup> Acurian states that it connects interested individuals that meet the eligibility requirements for a particular clinical trial with doctors overseeing the trial, which the Food and Drug Administration (FDA) requires to approve a drug for sale to the public.<sup>13</sup> Acurian notes that its matching services are "focused and inherently selective" and that it "often turns down requests to participate in trials when the individual would be a poor match or otherwise would not qualify for the trial."<sup>14</sup>

7. Acurian argues that its prerecorded calls should be exempt from the TCPA's restrictions on calls to residential lines as the calls are not made for a commercial purpose because they "do not, and are not intended to, encourage the called party to engage in a commercial transaction"<sup>15</sup> and "are analogous to the pure 'research' calls that the Commission has twice deemed to be exempt."<sup>16</sup> Alternatively, Acurian argues that its prerecorded calls do not include "advertisements" or constitute "telemarketing" as those terms are defined in the Commission's rules because they "do not make any mention of 'property, goods, or services' offered for sale by Acurian or its clients—and they certainly do not 'advertise' or 'encourage the purchase' of any such property, goods, or services."<sup>17</sup> It states that the purpose of these calls "is to match qualified individuals to clinical drug trials, not to advertise or encourage the purchase of any good or service."<sup>18</sup> Acurian further argues that granting the Petition would serve the public interest as it would "stamp out the threat of class action litigation based on [such] communications" and would facilitate compliance with FDA regulations.<sup>19</sup> Finally, Acurian maintains

---

<sup>11</sup> Petition at 1.

<sup>12</sup> *Id.* at 3-4.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.* at 5. Acurian states that "[i]f the individual is interested and meets the eligibility requirements for the particular trial, Acurian refers him or her to doctors who are participating in the trial. Where doing so is consistent with the recruitment rules established for the target study, Acurian will complete the call by requesting the individual's specific consent to be called again about future trials; if he or she declines to grant such consent, Acurian will no longer contact that individual." *Id.* at 4.

<sup>15</sup> *Id.* at 9.

<sup>16</sup> *Id.* at 9-10 (citing *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CC Docket No. 92-90, Report and Order, 7 FCC Rcd 8752, 8774, para. 41 (1992) (*1992 TCPA Order*) and *2012 TCPA Order*, 27 FCC Rcd at 1841, para. 28).

<sup>17</sup> *Id.* at 10-11 (quoting in part the definitions of "advertisement" and "telemarketing" in the Commission's rules, 47 CFR §§ 64.1200(f)(1), (12)).

<sup>18</sup> *Id.* at 11.

<sup>19</sup> *Id.* at 13-14. Acurian notes that it is the defendant in a putative class action lawsuit in California seeking millions of dollars in damages under the TCPA's prohibition on prerecorded calls. *See id.* at 5 (citing *Blotzer v. Acurian, Inc.*, No. 2:13-cv-3438-SVW-MAN (C.D. Cal. complaint filed May 14, 2013)). It appears that the lawsuit was settled and was ultimately dismissed. *See Blotzer v. Acurian, Inc.*, No. 2:13-cv-3438-SVW-MAN, Order (C.D. Cal. Apr. 8, 2014). We nevertheless exercise our discretion to respond to the Petition to address these calls, which we expect to be instructive for similar callers and consumers who receive such calls.

that the clarification it seeks is consistent with the First Amendment and that a contrary interpretation would fail strict scrutiny review.<sup>20</sup>

8. The Consumer and Governmental Affairs Bureau sought comment on Acurian's request.<sup>21</sup> Two individuals filed comments on the Petition.<sup>22</sup> One argues that Acurian's calls are commercial and would qualify for an exemption "[i]f the content was just about seeking test subjects and nothing more," but that the Commission should not entertain a "forum shopping" request from the target of a class action lawsuit.<sup>23</sup> The other commenter says the exemption Acurian seeks is "so broad that it would easily be exploited by others" and recommends that the Commission adopt a "case-by-case" approach.<sup>24</sup>

### III. DISCUSSION

9. Based on the facts described by Acurian and Commission rules and precedent, we grant Acurian's Petition and clarify that a call made using an artificial or prerecorded voice to a residential telephone line for the sole purpose of identifying individuals to participate in a clinical drug trial, where the call does not include any advertisement or telemarketing, is exempt from the Commission's prior-express-written-consent requirement.

10. As an initial matter, we conclude that we need not reach the issue of whether Acurian's calls are made for a commercial purpose to resolve the Petition. Even assuming, *arguendo*, that Acurian's calls are commercial in nature, we find they are nevertheless exempt from the prior-express-written-consent requirement because they do not include or introduce an advertisement or constitute telemarketing.<sup>25</sup> The Commission's rules define an "advertisement" as "any material advertising the commercial availability or quality of any property, goods, or services."<sup>26</sup> Our rules define "telemarketing" to mean "the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person."<sup>27</sup>

11. We agree with Acurian that its calls are not "advertising" or "telemarketing" because they do not identify property, goods, or services offered for sale by Acurian or its clients.<sup>28</sup> Acurian argues that its calls do not convey any information about the commercial availability of goods or services and do not solicit payment from the individuals it contacts.<sup>29</sup> Acurian further states that, until the FDA

---

<sup>20</sup> Petition at 14-16.

<sup>21</sup> See *Consumer and Governmental Affairs Bureau Seeks Comment on Petition for Declaratory Ruling Filed by Acurian, Inc.*, CG Docket No. 02-278, Public Notice, 29 FCC Rcd 1829 (CGB 2014).

<sup>22</sup> See Comment and Reply filed by Robert Biggerstaff; Comment filed by Gerald Roylance. The "Reply" filed by Roylance was filed on the comment deadline set in the public notice; thus, we have labeled it as a "Comment."

<sup>23</sup> Comment filed by Gerald Roylance at 1, 2, 4.

<sup>24</sup> Reply filed by Robert Biggerstaff at 1, 2-3.

<sup>25</sup> 47 CFR § 64.1200(a)(3)(iii). Our clarification is limited to the calls Acurian describes. Consequently, we disagree that the clarification will result in a "proliferation" of robocall abuses, as one commenter argues. See Reply filed by Robert Biggerstaff at 1, 2-3.

<sup>26</sup> 47 CFR § 64.1200(f)(1).

<sup>27</sup> *Id.* § 64.1200(f)(12).

<sup>28</sup> Petition at 10-11.

<sup>29</sup> *Id.* at 4.

approves a study drug, it is illegal to market or sell that drug in the United States, and Acurian's calls therefore do not involve the solicitation or marketing of any product or service.<sup>30</sup>

12. Based on the text of the Commission's existing rules and Acurian's description of its prerecorded message calls, we find that such calls do not include or introduce an advertisement or constitute telemarketing. The sole aim of Acurian's calls appears to be to encourage the called party to participate in an FDA-mandated clinical trial. Acurian states that its calls identify consumers suited for particular pharmaceutical trials and at no time are consumers asked to purchase any product or service, and there is nothing in the record that counters Acurian on those points. Nor does Acurian couple its offer to reimburse individuals for their time participating in the trial or free participation in a trial with any other offer or marketing effort to sell anything. Although the Commission has stated that offers for free goods or services that are part of an overall marketing campaign to sell property, goods, or services constitute "advertising the commercial availability or quality of any property, goods, or services"<sup>31</sup> and has raised concerns about so-called "dual purpose" calls,<sup>32</sup> we find that the calls at issue here do not fall into either of those categories.

13. Our ruling is consistent with Commission precedent. The Commission has made clear, for example, that calls by real estate agents representing a potential buyer to someone who has advertised their property for sale do not constitute "telephone solicitations" under the TCPA and Commission do-not-call requirements, so long as the purpose of the call is simply to discuss a potential sale of the property to the represented buyer.<sup>33</sup> As with Acurian's calls, those calls did not "encourage the called party to purchase, rent or invest in property."<sup>34</sup> Put simply, the caller was not trying to sell the consumer anything (even if the call might be on behalf of someone who might ultimately try to do so).

14. Similarly, our ruling is consistent with Commission precedent that a recruiter's call to discuss potential employment or service in the military with a consumer is not a "telephone solicitation" to the extent the called party will not be asked during or after the call to purchase, rent or invest in property, goods or services.<sup>35</sup> Acurian's calls are similar to these recruitment calls in that Acurian's calls are merely seeking to inform the called party about a drug trial and potentially to recruit that called party to serve in such a trial, rather than asking the called party to purchase, rent or invest in property, goods or services.

15. Further, courts have consistently interpreted the phrase "commercial availability" in the TCPA as tied to the offering of a good or service for sale,<sup>36</sup> and thus have found that messages seeking

---

<sup>30</sup> Petition at 11 (citing 21 U.S.C. § 355(a) ("No person shall introduce or deliver for introduction into interstate commerce any new drug, unless an approval of an application filed pursuant to subsection (b) or (j) is effective with respect to such drug."); 21 CFR §§ 314.1 *et seq.* (setting forth application procedures for obtaining FDA approval to market and sell new drugs)).

<sup>31</sup> 2003 *TCPA Order*, 18 FCC Rcd at 14907, para. 140 (citing 47 U.S.C. § 227(a)(4)).

<sup>32</sup> The Commission provided as examples: calls from mortgage brokers to their clients notifying them of lower interest rates, calls from phone companies to customers regarding new calling plans, or calls from credit card companies offering overdraft protection to existing customers. *Id.* at 14098-99, para. 142.

<sup>33</sup> See 2005 *TCPA Order*, 20 FCC Rcd at 3793-94, para. 15. "Telephone solicitation" (which was the subject of that case) and "telemarketing" (which is the subject of this one) have similar definitions in our rules. Namely, both include "the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person." 47 CFR § 64.1200(f)(12), (14).

<sup>34</sup> 2005 *TCPA Order*, 20 FCC Rcd at 3793-94, para. 15.

<sup>35</sup> See *id.* at 3794, para. 15, n.39.

<sup>36</sup> See, e.g., *Sandusky Wellness Ctr., LLC v. Medco Healthcare Solutions, Inc.*, 788 F.3d 218, 222 (6th Cir. 2015) (interpreting the definition of "advertisement" in the TCPA to require that "the fax must promote goods or services

(continued...)

individuals to participate in research trials or studies are not “advertisements” as defined by the statute.<sup>37</sup> Courts have also held that robocalls, text messages, or faxes that provide only information on employment opportunities do not constitute “advertisements” as they are not “advertising the commercial availability or quality of any property, goods, or services.”<sup>38</sup>

16. Finally, we recognize the importance of pharmaceutical trials, especially at a time when researchers search for therapeutics and vaccines to treat or prevent COVID-19. And, while some consumers may welcome the calls and the opportunity to participate in such trials, some may not. We note that, based on these concerns, the Commission recently limited calls for a commercial purpose where the calls do not include advertising or telemarketing to three calls within any consecutive 30-day period and required callers to allow consumers to opt out even before callers reach that limit.<sup>39</sup> We also take this opportunity to again emphasize that unscrupulous callers should not view this clarification as a retreat from the Commission’s aggressive work to combat illegal robocalls. As the COVID-19 pandemic continues to impact the United States, phone scammers have seized the opportunity to prey upon consumers. We are aware that consumers continue to receive telemarketing and fraudulent robocalls related to the pandemic.<sup>40</sup> As we have expressed repeatedly, we will be vigilant in monitoring complaints about these calls and will not hesitate to enforce our rules when appropriate.

17. For the reasons stated above, we find that the messages Acurian describes are not “advertisements” and do not constitute “telemarketing” as those terms are defined in the Commission’s rules.<sup>41</sup> We therefore grant Acurian’s Petition.<sup>42</sup>

(Continued from previous page) \_\_\_\_\_  
to be bought or sold”); *N.B. Indus., Inc. v. Wells Fargo & Co.*, 465 Fed. Appx. 640, 642 (9th Cir. 2012) (“To be commercially available within the meaning of [the Junk Fax Prevention Act], a good or service must be available to be bought or sold (or must be a pretext for advertising a product that is so available),” citing a dictionary definition of “commerce” as the “buying and selling of goods.”); see also *Florence Endocrine Clinic, PLLC v. Arriva Med., LLC*, 858 F.3d 1362, 1366-67 (11th Cir. 2017) (following *Sandusky* and assessing whether the faxes in question “promote the sale” of a product).

<sup>37</sup> See, e.g., *Ameriguard, Inc. v. Univ. of Kan. Med. Ctr. Research Inst.*, No. 06-0369-CV-W-ODS, 2006 WL 1766812 (W.D. Mo. June 23, 2006), *aff’d*, 222 Fed. Appx. 530 (8th Cir. 2007) (holding that a fax seeking recruits for a clinical research trial was not an advertisement under the TCPA); *Phillips Randolph Enters., LLC v. Adler-Weiner Research Chi., Inc.*, 526 F. Supp. 2d 851, 853 (N.D. Ill. 2007) (holding that a fax seeking participants for a research discussion on a new healthcare program was not an advertisement under the TCPA).

<sup>38</sup> See, e.g., *Gerrard v. Acara Solutions, Inc.*, 469 F.Supp.3d 96, 99 (W.D.N.Y. 2020) (text messages regarding a job opportunity); *Reardon v. Uber Techs., Inc.*, 115 F. Supp.3d 1090, 1096-97 (N.D. Cal. 2015) (text messages seeking to recruit Uber drivers); *Friedman v. Torchmark Corp.*, No. 12-CV-2837-IEG (BGS), 2013 WL 4102201 at \*5-6 (S.D. Cal. Aug. 13, 2013) (robocalls announcing a recruiting webinar); *Lutz Appellate Servs., Inc. v. Curry*, 859 F. Supp. 180, 181-82 (E.D. Pa. 1994) (faxes regarding a job opportunity).

<sup>39</sup> *2020 TCPA Exemptions Order*, at paras. 28-29.

<sup>40</sup> See *Rules and Regulations Implementing the Consumer Protection Act of 1991*, CG Docket No. 02-278, Declaratory Ruling, 35 FCC Rcd 2840, 2842, para. 10 (CGB 2020) (citing Federal Communications Commission, *COVID-19 Consumer Warnings and Safety Tips* <https://www.fcc.gov/covid-scams>).

<sup>41</sup> We decline to make any determination about the specific contours of the TCPA’s private right of action. See Petition at 13. We also do not address Acurian’s First Amendment argument as we conclude that its calls are not restricted by the TCPA’s prior-express-consent requirement.

<sup>42</sup> As discussed above, this declaratory ruling is based on Acurian’s general description of its calls and does not address the lawfulness of any specific calls made by Acurian, which did not include in the record either transcripts or detailed descriptions of such calls.

**IV. ORDERING CLAUSES**

18. **IT IS ORDERED** that, 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 Commission's rules, 47 CFR §§ 0.141, 0.361, the Petition for Declaratory Ruling filed by Acurian, Inc., on February 5, 2014, **IS GRANTED**.

19. **IT IS FURTHER ORDERED** that this Declaratory Ruling **SHALL BE EFFECTIVE** upon release.

FEDERAL COMMUNICATIONS COMMISSION

Patrick Webre  
Chief  
Consumer and Governmental Affairs Bureau

---

# Presidential Documents

---

Title 3—

Executive Order 13994 of January 21, 2021

The President

## Ensuring a Data-Driven Response to COVID-19 and Future High-Consequence Public Health Threats

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1. Policy.** It is the policy of my Administration to respond to the coronavirus disease 2019 (COVID-19) pandemic through effective approaches guided by the best available science and data, including by building back a better public health infrastructure. This stronger public health infrastructure must help the Nation effectively prevent, detect, and respond to future biological threats, both domestically and internationally.

Consistent with this policy, the heads of all executive departments and agencies (agencies) shall facilitate the gathering, sharing, and publication of COVID-19-related data, in coordination with the Coordinator of the COVID-19 Response and Counselor to the President (COVID-19 Response Coordinator), to the extent permitted by law, and with appropriate protections for confidentiality, privacy, law enforcement, and national security. These efforts shall assist Federal, State, local, Tribal, and territorial authorities in developing and implementing policies to facilitate informed community decision-making, to further public understanding of the pandemic and the response, and to deter the spread of misinformation and disinformation.

**Sec. 2. Enhancing Data Collection and Collaboration Capabilities for High-Consequence Public Health Threats, Such as the COVID-19 Pandemic.** (a) The Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Labor, the Secretary of Health and Human Services (HHS), the Secretary of Education, the Director of the Office of Management and Budget (OMB), the Director of National Intelligence, the Director of the Office of Science and Technology Policy (OSTP), and the Director of the National Science Foundation shall each promptly designate a senior official to serve as their agency's lead to work on COVID-19- and pandemic-related data issues. This official, in consultation with the COVID-19 Response Coordinator, shall take steps to make data relevant to high-consequence public health threats, such as the COVID-19 pandemic, publicly available and accessible.

(b) The COVID-19 Response Coordinator shall, as necessary, convene appropriate representatives from relevant agencies to coordinate the agencies' collection, provision, and analysis of data, including key equity indicators, regarding the COVID-19 response, as well as their sharing of such data with State, local, Tribal, and territorial authorities.

(c) The Director of OMB, in consultation with the Director of OSTP, the United States Chief Technology Officer, and the COVID-19 Response Coordinator, shall promptly review the Federal Government's existing approaches to open data, and shall issue supplemental guidance, as appropriate and consistent with applicable law, concerning how to de-identify COVID-19-related data; how to make data open to the public in human- and machine-readable formats as rapidly as possible; and any other topic the Director of OMB concludes would appropriately advance the policy of this order. Any guidance shall include appropriate protections for the information described in section 5 of this order.

(d) The Director of the Office of Personnel Management, in consultation with the Director of OMB, shall promptly:

(i) review the ability of agencies to hire personnel expeditiously into roles related to information technology and the collection, provision, analysis, or other use of data to address high-consequence public health threats, such as the COVID-19 pandemic; and

(ii) take action, as appropriate and consistent with applicable law, to support agencies in such efforts.

**Sec. 3. *Public Health Data Systems.*** The Secretary of HHS, in consultation with the COVID-19 Response Coordinator and the heads of relevant agencies, shall promptly:

(a) review the effectiveness, interoperability, and connectivity of public health data systems supporting the detection of and response to high-consequence public health threats, such as the COVID-19 pandemic;

(b) review the collection of morbidity and mortality data by State, local, Tribal, and territorial governments during high-consequence public health threats, such as the COVID-19 pandemic; and

(c) issue a report summarizing the findings of the reviews detailed in subsections (a) and (b) of this section and any recommendations for addressing areas for improvement identified in the reviews.

**Sec. 4. *Advancing Innovation in Public Health Data and Analytics.*** The Director of OSTP, in coordination with the National Science and Technology Council, as appropriate, shall develop a plan for advancing innovation in public health data and analytics in the United States.

**Sec. 5. *Privileged Information.*** Nothing in this order shall compel or authorize the disclosure of privileged information, law-enforcement information, national-security information, personal information, or information the disclosure of which is prohibited by law.

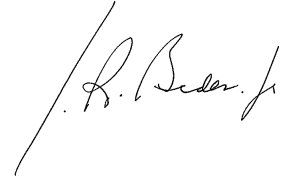
**Sec. 6. *General Provisions.*** (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,  
*January 21, 2021.*





U.S. Department of Health and Human Services

# Artificial Intelligence (AI) Strategy

January 2021



## Table of Contents

<b>1.HHS Mission &amp; AI Ambition .....</b>	<b>2</b>
<b>2.Strategic Approach.....</b>	<b>3</b>
2.1 Leading Health and Human Services AI Innovation .....	3
2.2 Partnering and Responding to AI-Driven Approaches within the Health Ecosystem .....	3
<b>3.Execution and Governance.....</b>	<b>4</b>
3.1 AI Council & AI Community of Practice .....	4
3.2 Enabling Focus Areas.....	5
<b>4. Conclusion.....</b>	<b>7</b>



## 1. HHS Mission & AI Ambition

The Department of Health and Human Services (HHS) serves to enhance the health and well-being of all Americans, by providing for effective health and human services and by fostering sound, sustained scientific advances in medicine, public health, and social services. This mission, supported by and connected to the missions of its partners, including state, local, tribal and territorial (SLTT) governments, requires HHS to continue to align Department efforts and priorities to address the evolving health and human services needs of the Nation.

HHS plays a variety of critical roles within this shared mission, serving as, for example, a regulator of the health industry, purchaser of healthcare, catalyst for innovation in the delivery of health and human services, investor of grant and research funding, and convener of common interests and priorities for ensuring the health and wellbeing well-being for all Americans. As the Department builds upon its current capabilities and adapts to a changing environment and emerging technology, HHS recognizes that Artificial Intelligence (AI) will be a critical enabler of its mission in the future. An enterprise AI strategy will provide direction and guidance in achieving the Department's AI ambition:

*Together with its partners in academia, industry and government, HHS will leverage AI to solve previously unsolvable problems by **continuing to lead advances in the health and wellbeing** of the American people, **responding to the use of AI** across the health and human services ecosystem, and **scaling trustworthy AI adoption** across the Department.*

To achieve HHS's ambition, this enterprise AI strategy will set forth an approach and focus areas intended to encourage and enable Department-wide familiarity, comfort, and fluency with AI technology and its potential (AI adoption), the application of best practices and lessons learned from piloting and implementing AI capabilities to additional domains and use cases across HHS (AI scaling), and increased speed at which HHS adopts and scales AI (AI acceleration).

AI refers to the theory and development of computer systems able to perform tasks normally requiring human intelligence, in order to deliver solutions that can automate routine tasks, draw data-based insights, or augment human activities. HHS has already made advances in the use of AI, for example, the Food and Drug Administration (FDA) has been developing a regulatory framework for AI/Machine Learning (ML)-driven software modifications to provide appropriate safety and effectiveness guidelines, and the National Institutes of Health (NIH) has collaborated and invested in AI-based projects to discover health solutions across research and medical settings, including analysis of biomedical imaging to diagnose diseases such as COVID-19. HHS' efforts to date demonstrate its desire and commitment to fully realize the benefits of AI. Given the immense potential for AI to improve health and human services, HHS will leverage AI capabilities to solve complex mission challenges and generate AI-enabled insights to inform efficient programmatic and business decisions, while removing barriers to AI innovation.

The strategy of the Department is aligned with the commitment of the Federal Government to "promote the use of trustworthy AI" (Executive Order 13960) and to "maintain American leadership in AI" (Executive Order 13859) in both its own Departmental activities and the



broader health and human services ecosystem.

## 2. Strategic Approach

### 2.1 Leading Health and Human Services AI Innovation

HHS will prioritize the application and development of AI across common enterprise mission areas in which the Department serves as a lead in health and human services innovation. HHS Divisions will continue to lead in identifying opportunities for mission-driven AI solutions, mitigating risks appropriately, against a shared framework of federal and Departmental guidance. Key HHS and Division missions include:

#### *Regulating and overseeing the use of AI in the health industry*

HHS' regulatory responsibility spans all aspects of healthcare including standards for healthcare delivery, payments, medical device software, medical products and food, and privacy to ensure compliance, safety, and effectiveness. AI can be leveraged to reduce regulatory burdens and streamline processes that accelerate advancements in the health and wellbeing of Americans. To harness these benefits, HHS will continue to develop standards that inform policy and guidance for safe and transparent AI use and encourage agile and adaptable innovation.

#### *Funding programs, grants, and research that leverage AI-based solutions to deliver outcomes*

As the largest grant-making agency in the federal government, HHS evaluates and oversees grants supporting thousands of projects that invest in research and deliver services in support of its mission. As a steward of federal funds, HHS will encourage grant recipients to consider AI's utility and prioritize and enable programs, grants, and research that use AI in trustworthy ways in order to more efficiently or effectively realize mission impact. Specifically, these efforts include, but are not limited to, advancing biomedicine through AI-enabled insights into large datasets, predictive analytics in public health surveillance and responses, and advancing the use of cognitive technologies to identify new approaches to health and behavioral conditions with complex multifactorial causality. HHS will also deploy AI in the grantmaking process itself, for example, to facilitate risk-based review of grants, in order to optimize the allocation of resources and to reduce (detect, prevent, mitigate) opportunities for waste, fraud, and abuse of federal funds.

### 2.2 Partnering and Responding to AI-Driven Approaches within the Health Ecosystem

HHS will prioritize the application and development of AI across common enterprise mission areas that enable the Department to respond to the dynamic, shared needs of various partners in health and human services innovation, including:

#### *Collaborating with internal partners, external partners, including academia, the private sector, and SLTT governments, to enhance programs and services through the potential of AI*

HHS collaborates across Divisions and with partners in private industry, academia, and various SLTT governments to advance common interests across shared missions in administering essential human services and health programs. The Department will engage with these partners



to identify opportunities for AI applications that advance health and human services, including streamlining processes that span the Department and its partners, reducing costly or inefficient resources allocated to low-value, repetitive tasks, and providing enhanced experiences and services for program beneficiaries and the American public. The Department will also engage with partners to prioritize needs and opportunities for AI advancements that enable better outcomes in research, improve clinical practice, public health and safety, social services, disease prevention, and wellness.

*Identifying gaps and unmet needs in health and scientific areas that would benefit from government involvement and AI application*

HHS continually strives to identify and pursue opportunities utilizing individual and population health data to improve the public health of Americans. This vast knowledge and data pave the way for AI-based solutions to better understand trends, outcomes, and opportunities across the health and human services ecosystem. HHS, at the enterprise level, will position itself to facilitate public-private partnerships (PPP), including those that may be implemented at the HHS Division level. It is anticipated that these partnerships will be one among several approaches that can link AI technology with the support necessary for success: (1) external and governmental expertise engaged in mutual dialogue, (2) external and governmental datasets, models, and algorithms appropriately shared, interlinked, and leveraged for insight, (3) policy support and risk-based oversight tied to the E.O. 13960 principles for trustworthy AI, and (4) well-defined use cases tied to the advancement of health and welfare, with clear criteria for success, interoperability, and reuse.

### 3. Execution and Governance

#### 3.1 AI Council & AI Community of Practice

To effectively advance the AI ambition outlined in this strategy, the HHS AI Council will be established to support AI governance, strategy execution, and development of strategic AI priorities across the enterprise. The AI Council has complementary objectives to:

- I. Communicate and champion the Department's AI vision and ambition
- II. Execute and govern the implementation of the enterprise AI strategy and key strategic priorities to scale AI across the Department

In support of these objectives, the HHS AI Council will:

*Set and Execute Priorities.* As the champion of the Department AI Strategy, the HHS AI Council is responsible for translating strategic objectives to identify and refine enterprise AI priorities, as well as oversee the execution of the Enterprise AI Strategy. The AI Council will communicate Department AI priorities to enable Operating and Staff Divisions to scale AI adoption in key mission areas. To ensure progress in AI priorities, the Council will develop and leverage performance plans, implementation timelines, and key performance indicators (KPIs) to drive accountability. The AI Council will report annually on this progress and communicate a



developed report to the Secretary and the HHS Management Council.

*Cultivate Partnerships.* The AI Council will convene AI interests across the Department and the health and human services ecosystem to advance and better outcomes in healthcare, research, and SLTT government missions. The AI Council will identify and foster relationships with public and private entities aligned to priority AI initiatives, as well as promote collaboration across partnerships to develop AI innovations.

*Provide Governance Support.* The AI Council will align HHS' AI governance approach and implementation planning across strategic objectives including the White House and other federal AI guidance. The AI Council will collaborate with existing Department governance forums, as well as other federal government oversight offices, to advance the Department's AI ambition in accordance with the objectives of the American AI Initiative.

*Sponsor a Community of Practice.* The AI Council will establish and support a Community of Practice (CoP) comprised of AI practitioners – such as data scientists, machine learning experts, mathematicians, system developers, computer programmers, solution architects, and other technologists, as well as the health scientists and program leaders who employ AI within their projects and organizations – at all employee levels across Divisions. While the AI Council is responsible for translating and identifying Department AI priorities, the AI CoP will align Department priorities to the efforts of AI practitioners across Divisions to support scaling of AI pilots and use cases. The AI Council, recognizing the importance of dedicated resources, will identify and provide required resources to ensure effective CoP support for enterprise-wide AI adoption.

The CoP will foster enterprise-wide AI adoption by sharing lessons learned, identifying AI opportunities, providing peer recommendations for scaling AI use cases, and supporting shared access to AI tools, resources, innovation labs, and best practices. Members of the Community of Practice may elect to support Work Groups, established by the AI Council, to activate and drive priority AI initiatives across the Department.

### **3.2 Enabling Focus Areas**

The AI Council will identify and support priority activities within key focus areas that will accelerate AI adoption and scaling across HHS divisions, such as developing an AI use case inventory to catalogue active and planned AI use cases, fostering new public and private partnerships to drive AI innovation, and establishing best practices and recommendations for trustworthy and ethical AI use to adhere to federal and ethical guidelines, as well as federal civil rights laws, including conscience and religious liberty provisions.

To enable Divisions to apply, advance, and invest in trustworthy AI solutions across key mission areas, the AI Council will invest in and align enterprise-level support to four (4) key focus areas:

*Develop an AI-ready Workforce and Strengthen AI Culture.* Leveraging AI to solve previously unsolvable problems requires domain expertise, as well as a degree of AI fluency, to identify





relevant AI technologies and techniques that can address a given problem set or process. It also requires a workforce that is aware of, and comfortable with, the potential of AI and how it is being used by its organization. HHS will (1) cultivate AI fluency and skillsets to enhance scientific expertise and accelerate the Department's ability to develop innovative solutions across health and human services, (2) support a culture of rigor, collaboration and innovation to ensure successful scaling of AI solutions by communicating Department AI priorities and projects and promoting AI awareness, and (3) increase adoption by focusing on broad, Department-wide awareness of the potential of AI, provide regular communications that inform employees of how AI is being used, and bring visibility to available AI trainings and workshops that enable practitioners to more readily learn about AI and apply those learnings to their domain of expertise, creating an opportunity for all HHS employees to play a role in identifying relevant use cases and potential applications.

*Encourage Health AI Innovation and Research & Development (R&D).* Advancing health and human services outcomes and research with AI will require continuous convening of missions and unmet needs across academia, private sector, and SLTT governments. The Department will foster new partnerships to identify critical AI priorities and emerging AI innovations across health and human services. The Department will communicate these shared priorities with Divisions to inform, accelerate, and guide research grant investments, and ultimately advance shared health and human services mission outcomes. The Department will also track internal AI initiatives and prioritize AI applications that enable overall advancements in the health and well-being of Americans.

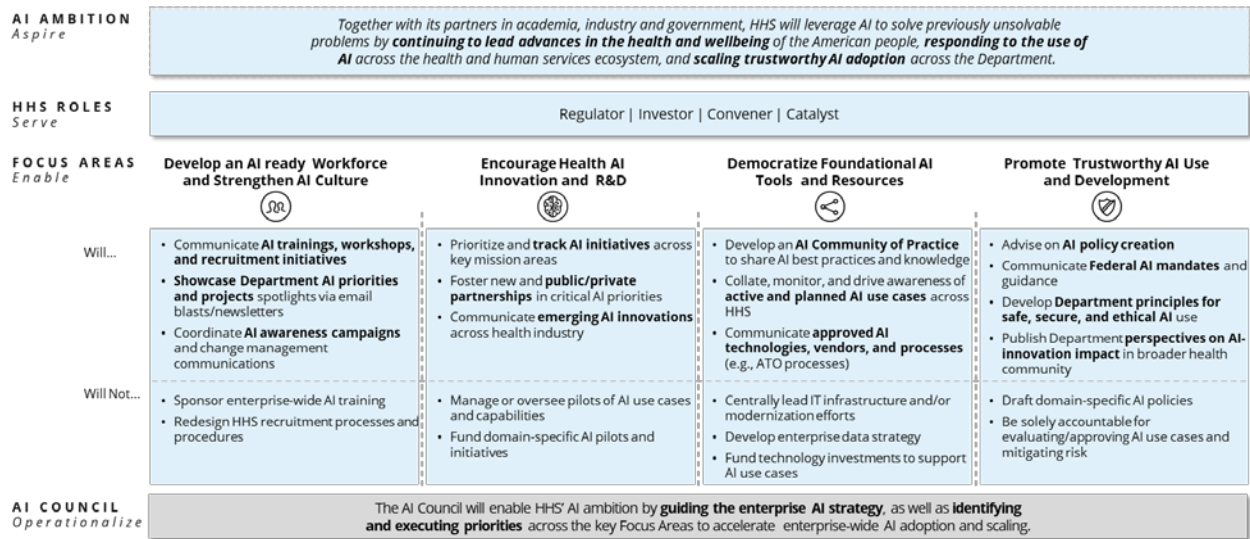
*Democratize Foundational AI Tools and Resources.* Readily accessible tools, data assets, resources, and best practices will be critical to minimizing duplicative AI efforts, increasing reproducibility, and ensuring successful enterprise-wide AI adoption. To accelerate scaling of cross-Division AI use cases, the enterprise will promote access to AI resources and tools, as well as drive awareness of current and planned AI use cases across HHS. The Department will leverage the established AI Community of Practice to further develop a common understanding of AI, share AI expertise across Divisions, and communicate and promote effective AI technologies, vendors, and processes.

*Promote Ethical, Trustworthy AI Use and Development.* Inspiring trust and confidence in AI use, internally and across the health and human services ecosystem, will be of paramount importance to successful AI adoption. The Department will translate federal directives outlined in Executive Order 13960 to support Divisions in deploying reliable, explainable, non-biased, and secure AI systems that respect citizens' privacy and data security. The enterprise will support Divisions in developing policies that ensure transparency and accountability in AI use by communicating Department-specific principles for effective, equitable, safe, secure, and ethical AI and data used to create and operate AI. The Department will also promote and support the application of existing cybersecurity frameworks to AI use cases across Divisions. The Department will also promote the evaluation of applied AI for accuracy, effectiveness, and health equity.



Successfully accelerating AI adoption will require a coordinated effort across the Divisions. The Department will continue to enable Operating and Staff Divisions to manage and oversee critical AI activities within their respective domains, such as implementing AI pilots and initiatives, developing domain-specific policies and regulations, evaluating AI use cases and mitigating risk, and furthering an AI-ready workforce and collaborative culture.

**Figure 3.2: HHS Enterprise AI Strategy Summary**

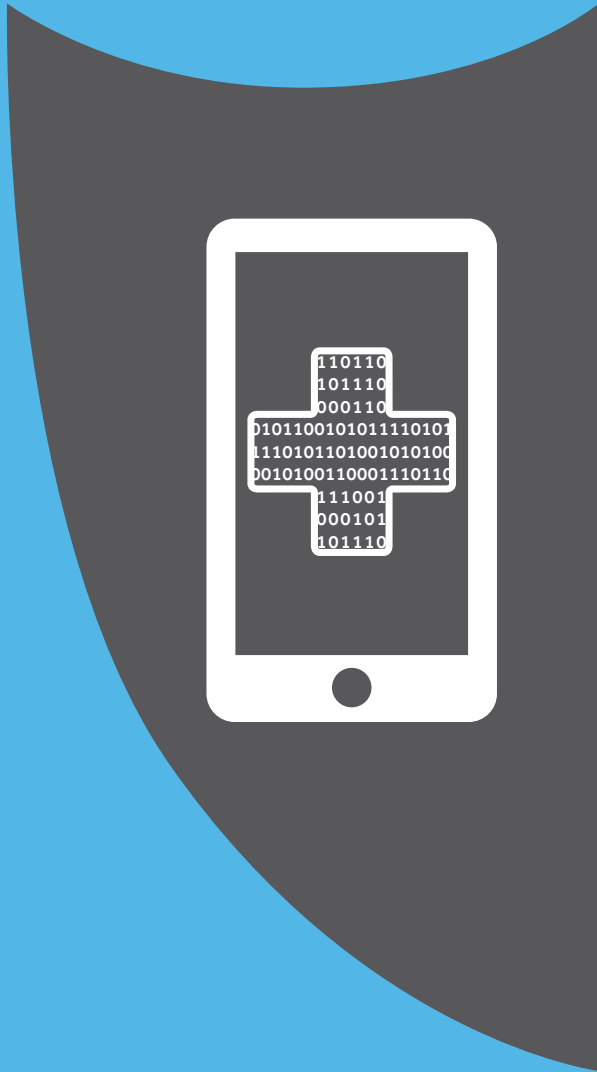


## 4. Conclusion

HHS must continue its leadership at the vanguard of health and human services innovation to meet the dynamic needs of the American people. Trustworthy, ethical, and intentional use of AI technologies will accelerate HHS' ability to meet these evolving needs as both a leader and responsive partner in innovations across health and human services. AI will be critical to the Department in achieving its mission and vision, as well as positioning HHS to address the health and human services *challenges of today and tomorrow*.

Ultimately, this strategy is the first step towards transforming HHS into an AI fueled enterprise. This strategy lays the foundation upon which the AI Council can use to drive change across the Department by encouraging the application of AI to promote advances in the sciences, public health, and social services—improving the quality of life for all Americans.





# Proposed Consumer Privacy **FRAME- WORK** for Health Data

FEBRUARY 2021

## About Center for Democracy & Technology

The Center for Democracy & Technology is a 25-year-old nonprofit, non-partisan organization working to promote democratic values by shaping technology policy and architecture. For more information, visit [cdt.org](http://cdt.org).

## About eHealth Initiative & Foundation

eHealth Initiative & Foundation (eHI) convenes executives from every stakeholder group in healthcare to discuss, identify, and share best practices to transform the delivery of healthcare using technology and innovation. eHI, along with its coalition of members, focuses on education, research, and advocacy to promote the use and sharing of data to improve healthcare. Our vision is to harmonize new technology and care models in a way that improves population health and consumer experiences. eHI has become a go-to resource for the industry through its eHealth Resource Center. For more information, visit [ehidc.org](http://ehidc.org).

## Acknowledgements

This framework is made possible with the support of the Robert Wood Johnson Foundation, and with assistance from our Steering Committee.

Special thanks to members of our two work groups for their invaluable engagement help and for their guidance. A list of select Steering Committee members can be found in the [Appendix](#).

# Proposed Consumer Privacy Framework for Health Data

## Table of Contents

Executive Summary.....	4
Introduction and Background.....	4
Project Goals and Process.....	4
Value of This Proposal for Different Stakeholders.....	5
Substantive Standards and Policy Rationale.....	7
Definitions.....	7
Collection and Processing of Consumer Health Information.....	14
I. Obligations for Participating Entities.....	14
II. Consumer Controls.....	18
III. Notice and Transparency.....	21
IV. Consent.....	23
V. Exceptions.....	24
Proposed Self-Regulatory Program: Policy Rationale.....	28
Addressing Consumer Trust.....	28
Program Goals.....	29
Establishment of a New Self-Regulatory Program.....	29
Consumer and Participant Benefits.....	30
Incorporation of Feedback.....	30
Self-Regulatory Program for Non-HIPAA Healthcare Data.....	31
Appendix.....	33
Steering Committee Members.....	33

---

# Executive Summary

## Introduction and Background

Health data—or data used for health-related purposes—is not regulated by a single national privacy framework. Since 1996, the Health Insurance Portability and Accountability Act (HIPAA) has governed the use and disclosure of certain health information held by certain entities such as doctors and insurance companies. However, with the rise of wearable devices, health and wellness apps, online services, and the Internet of Things, extraordinary amounts of information reflecting mental and physical well-being are created and held by entities that are not bound by HIPAA obligations. This issue has only gained importance, as new regulations finalized in the spring of 2020 will also ease and promote the movement of previously HIPAA-covered medical records into this commercially facing, non-HIPAA-covered and unregulated space.<sup>1</sup> The novel coronavirus has also thrust the issue of patient data privacy to the forefront, as efforts to trace and combat the spread of the virus have brought with them the relaxation of some federal privacy protections as well as increased data collection and use.

## Project Goals and Process

With funding from the Robert Wood Johnson Foundation, the eHealth Initiative (eHI) and the Center for Democracy & Technology (CDT) collaborated on a Consumer Privacy Framework for Health Data, with invaluable engagement and help from a steering committee of leaders from healthcare entities, technology companies, academia, and organizations advocating for privacy, consumer, and civil rights.

This steering committee helped guide eHI and CDT during the development of this framework. Specifically, the framework consists of a set of detailed use, access, and disclosure principles and controls for health data that are designed to address the gaps in legal protections for health data outside HIPAA's coverage. The framework also includes a proposed self-regulatory program to hold companies accountable to such standards. Non-HIPAA-covered entities would voluntarily hold themselves to a set of standards and subject themselves to potential enforcement mechanisms beyond current Federal Trade Commission (FTC) processes. Even outside this program, the authors hope that the substantive standards will serve as a benchmark to shape industry conduct and influence companies' approaches to ensure users' health data is protected.

---

<sup>1</sup> 85 Fed. Reg. 25642 (May 1, 2020) and 85 Fed. Reg. 25510 (May 1, 2020). For a comprehensive review of the current legal landscape governing health data and the gaps in protection for the same, please see Belfort, R., Dworkowitz, A., Bernstein, William S., Pawlak, B. and Yi, P. *A Shared Responsibility: Protecting Health Data Privacy in an Increasingly Connected World*, June 2020, available at [http://www.manatt.com/Manatt/media/Media/PDF/White%20Papers/Healthcare-Whitepaper-RWJF-Protecting-Consumer-Health-Data-Privacy-in-an-Increasingly-Connected-World\\_e.pdf](http://www.manatt.com/Manatt/media/Media/PDF/White%20Papers/Healthcare-Whitepaper-RWJF-Protecting-Consumer-Health-Data-Privacy-in-an-Increasingly-Connected-World_e.pdf) (Manatt White Paper).

The standards emphasize transparency, accountability, and appropriate limitations on health data collection, disclosure, and use. Importantly, the standards:

1. Move beyond outdated models that place too much emphasis on notice and consent and fail to articulate data use limits;
2. Cover all information that can be used to make inferences or judgments about a person's physical or mental health; and
3. Cover all non-HIPAA-covered entities that collect, disclose, or use consumer health information, regardless of the size or business model of the covered entity.

With respect to the self-regulatory program, the framework seeks to balance the need for enforcement mechanisms that will effectively hold companies responsible and promote consumer trust, while ensuring the program is workable enough for potential participating entities to join. This is a challenging balance, which the authors know will rely on entities participating in good faith.

Importantly, this proposal is **not** designed to be a replacement for new and necessary comprehensive data privacy legislation. Indeed, we believe strongly in the need for such a law and support all efforts to date that have served to build momentum for one. Given that congressional action is likely some time away and would take additional time to go into effect, this effort is designed to build support for best practices and enable us to take what action we can now, in the interim, to shore up protections for non-HIPAA-covered health data. We hope that some of the tenets of our proposal can and will be helpful to federal lawmakers in their future efforts.

## Value of This Proposal for Different Stakeholders

**Consumers.** This model raises the bar for consumer privacy. Some existing best practices and voluntary frameworks define health information quite narrowly and do not cover all the data that reflects mental or physical wellbeing or health. Many best practices are also often targeted at a specific type of app or service instead of all entities that collect and use health data. Our comprehensive proposal closes these gaps in coverage.

Substantively, our draft goes beyond outdated models that revolve primarily around notice and consent. While transparency and consent remain important elements within the framework, many of the core privacy-protecting provisions of this framework are focused on how consumer health information is collected, disclosed, and used. Although older laws or frameworks may have made sense in decades past, people can no longer make informed and timely decisions about all the different websites, apps, and devices they use every day given the proliferation in the number of available technologies and the length, details, and lack of clarity of their terms of service. By putting clear restrictions on the collection, disclosure, and use of data, the proposed framework shifts the burden of privacy risk off users and onto the companies.

Finally, because our model borrows the best concepts from Europe and California, users will benefit from the heightened protections developed in those regions even if their local laws have not been updated with more modern data privacy protections.

**Non-HIPAA-covered technology companies that collect health information.** Entities that elect to participate and adopt the framework will also benefit. First, they will stay ahead of the regulatory curve. By making pro-privacy decisions now, they will avoid having to make product changes that could be more expensive, time-consuming, or complicated in response to future regulation.

Second, while entities will be able to develop and offer the product a consumer requests, they will be deterred from collecting and using health data they do not actually need. This should reduce legal risks in a world where consumers and enforcement agencies expect more from companies that handle data. Participating entities may also see significant reputational and thus commercial benefit in an increasingly crowded market.

Finally, this model has the potential to provide some compliance certainty for participants. By adopting more forward-looking privacy practices, companies and organizations will avoid the gray or evolving areas of existing laws. Especially for smaller or newer companies having difficulty fully understanding their numerous federal and state legal obligations, which can often be unclear and/or conflicting, compliance with our framework's standards would provide some assurance that participants are staying ahead of various potential federal and state requirements.

**Regulators and oversight bodies.** Congress, the FTC and their state-level counterparts will benefit from companies committing to a common set of publicly available data practices. This commitment will allow these governmental bodies to enforce these practices, which will be more explicit than many existing company privacy policies. Instead of engaging in complicated investigations and balancing tests, these entities will be able to measure compliance more easily and better allocate their limited enforcement resources.

**Traditional healthcare system entities.** Finally, although this framework is geared toward companies that operate outside the traditional healthcare system and thus are not subject to the obligations and protections of HIPAA, our framework will benefit HIPAA-covered entities as well. The framework recognizes the importance of research and establishes clear standards for when research relying on consumer health information is permitted.

Moreover, the release of the Centers for Medicare & Medicaid Services and Office of the National Coordinator for Health Information Technology final rules regarding interoperability and information-blocking means that consumers will soon have greater access than ever to their own health data. By virtue of the framework, providers and consumers alike will have a far easier time choosing applications for this data transfer that adhere to meaningful and robust privacy practices.

# Substantive Standards and Policy Rationale

For any follow-up questions, kindly contact Andrew Crawford at CDT ([acrawford@cdt.org](mailto:acrawford@cdt.org)).

In addition to the text of the framework, throughout this section we include blue fields containing summaries of the feedback we received, policy rationale, and explanations for each section.

## Definitions

### 1. **Affirmative Express Consent**

- a. In general - The term “affirmative express consent” means an affirmative act by a consumer that clearly communicates the consumer’s authorization for an act or practice, in response to a specific request that:
  - i. Is provided to the consumer in a clear and conspicuous disclosure that is separate from other options or acceptance of general terms; and
  - ii. Includes a description of each act or practice for which the consumer’s consent is sought that:
    - (A) Is written concisely and in an easy-to-understand manner that is accessible to all consumers; and
    - (B) Includes clear headings that would enable a reasonable consumer to identify and understand the act or practice.
- b. Express consent required - Affirmative express consent shall not be inferred from the inaction of a consumer or the consumer’s continued use of a service or product.
- c. Voluntary - Affirmative express consent shall be freely given and nonconditioned.

Much of the data covered by this framework is inherently sensitive on its own or when used in certain ways. When the collection, use, or sharing of certain data is conditioned on consent, it is crucial that consent be meaningful. It has been repeatedly documented that terms that appear in lengthy privacy policies do not meet this standard. To that end, this definition requires the clear and thorough presentation of information to users and clarifies that consent cannot be inferred from consumer inaction. Moreover, consumer consent must be voluntary and cannot be conditioned (for example, with a condition that unnecessary data be collected as part of a sale). This approach is also consistent with the FTC’s approach, other frameworks, and bipartisan constructions of affirmative express consent introduced during the 116th Congress, including comprehensive privacy legislation and legislation that would cover consumer health information.

2. **Aggregated Health Data** - The term “aggregated health data” means health data that relates to a group or category of individuals but cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or a household.

A participating entity in possession of aggregated health data shall:

- a. Take reasonable measures to safeguard the aggregated health data from reidentification, including the adoption of technical and organizational measures to ensure that the information is not linked to any individual, household, or device used by an individual or a household;
- b. Publicly commit in a conspicuous manner not to attempt to reidentify or associate the aggregated health data with any individual, household, or device used by an individual or a household; and
- c. Contractually require the same commitments from recipients of all transfers of aggregated health data.

This framework recognizes that properly aggregated data may pose fewer privacy risks to individuals, families, and communities. As a result of that reduced privacy risk and the offsetting public benefit of some uses of aggregated data, this framework permits certain uses of aggregated data for research purposes or internal analysis (see Section V). Importantly, aggregation is not a silver bullet in protecting individual privacy. This framework requires covered entities to safeguard aggregated health data from reidentification and to contractually require the same commitment from any entity that receives the aggregated data.

We received comments asking for greater clarification around the definitions of both aggregated and de-identified data. It is critical for these definitions to be clear because aggregated and de-identified data sets are subject to different use limitations under the framework. To address these comments, the definitions of aggregated and de-identified health information have been modified to make clear that they are not subsets of consumer health information. Additional clerical edits have also been made to these definitions to ensure consistency of terms and approach.



3. **Consumer** - The term “consumer” means an individual, including minors.

Comments received about this section asked whether minors are included within the definition of consumer. Minors face the same potential harms when their health data is misused or used in unintended ways and should have the same protections as everyone else under the framework. To address this feedback, we have now included a reference to minors within the definition to clearly indicate that they are included.

4. **Consumer Health Information** - The term “consumer health information” means:

- a. Any information, recorded in any form or medium, that is created or received by an entity and:
  - i. Relates to or is used to determine, predict, or estimate the past, present, or future physical or mental health condition of an individual; or
  - ii. Relates to the provision of healthcare to an individual.
- b. The following data sets regardless of the purpose or outcome of the collection, disclosure, or use:
  - i. Genetic data;
  - ii. Data that reflects a particular disease or condition;
  - iii. Data that reflects any substance use disorder;
  - iv. Data that reflects reproductive health; and
  - v. Data that reflects disability.<sup>2</sup>
- c. Exclusions - Consumer health information does not include:
  - i. Protected health information (PHI) held or maintained by a HIPAA-covered entity or business associates acting for the covered entity.

<sup>2</sup> As defined under the Americans with Disabilities Act of 1990, available at <https://www.ada.gov/pubs/adastatute08.htm>.

This definition intentionally rejects previous notions of “health data” that are limited to the direct provision of health services by a professional. It also avoids the approach taken by some other voluntary frameworks that create a list of health conditions that qualify for protection. This definition instead focuses on the nature of the information and how it is used. It recognizes that all data can be “health data” if it is used for those purposes, even if it appears unrelated on its face. To that end, subsection (a) covers all data that a participant collects, shares, or uses for health purposes. Examples of some of these data sets are as follows:

- Data that reflects racial and ethnic origin;
- Biometric data; and
- Data that reflects sexual orientation.

Subsection (b) declares that certain sensitive health information shall always be subject to the framework, regardless of the context of its use.

A purpose- and use-based approach to this definition has several benefits. First, it benefits consumers by raising the bar for all the data that is used to impact their health and wellness. Modern data use is complex, opaque, and instantaneous. Trying to delineate distinct data sets as worthy of coverage and others as not no longer makes sense for the people whose information is implicated. Second, it creates a tech-neutral standard that will stay relevant as technology evolves.

We received a number of thoughtful and detailed comments about this section. Several of the comments focused on the broad nature of the definition. We took this feedback seriously. To address these points, the definition has been refined to clarify when certain data sets, such as racial and biometric data, will be treated as consumer health information. These edits focus the framework’s protections on data sets that are collected, disclosed, and used for health purposes while still recognizing that certain types of data are always consumer health information. Finally, the addition of the exclusion section is intended to make clear that this framework is focused on consumer health information that is not covered by HIPAA.

5. **De-identified Health Data** - The term “de-identified health data” means health data that cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or a household.

A participating entity in possession of de-identified health data shall:

- a. Take reasonable measures to safeguard the de-identified health data from reidentification, including the adoption of technical and organizational measures to ensure that the information is not linked to any individual, household, or device used by an individual or a household;
- b. Publicly commit in a conspicuous manner not to attempt to reidentify or associate the de-identified health data with any individual, household, or device used by an individual or a household; and
- c. Contractually require the same commitments from recipients of all transfers of the de-identified health data.

Properly de-identified data may pose fewer privacy risks to individuals, families and communities. As a result of that reduced privacy risk and the offsetting public benefit of some uses of de-identified health data, this framework permits certain uses of this data for research purposes or internal analysis (see Section V). De-identification is not a silver bullet in protecting individual privacy. This framework requires covered entities to safeguard de-identified health data from reidentification and to contractually require the same commitment from any entity that receives the de-identified data.

We received a number of comments about this definition that are discussed under the definition of aggregated health data above. Additionally, we received comments specifically about de-identified data. Those comments focused on de-identified health data carrying a greater potential to be reidentified compared to aggregated health data. While it is not possible to completely eliminate the risk of reidentification, the definition requires participating entities to not reidentify this data.

6. **Participating Entity** - The term “participating entity” means an entity that collects, gathers, or uses consumer health information in any form or medium for nonpersonal purposes and that adopts this framework.

This has been drafted broadly in an effort to capture all entities that collect and/or use consumer health information. It no longer makes sense for consumers to have different rights depending on what entities hold their information.

We received some comments seeking greater clarification regarding how this framework would apply to entities that may have certain data sets that are covered by HIPAA while others are not. This framework is focused on non-HIPAA-covered data and is intended to increase privacy protections around data sets that currently fall outside HIPAA’s coverage while not creating overlapping or conflicting requirements for participating entities.

7. **Privacy Review Board** - The term “privacy review board” means an independent board that:
- Is composed of at least three members;
  - Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual’s privacy rights and related interests;
  - Includes at least two members who are not affiliated with the participating entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities;
  - Includes at least one member who is a consumer representative with experience working in the consumer health context; and
  - Does not have any member participating in a review of any project in which the member has a conflict of interest.

For the purposes of this definition, an institutional review board (IRB) or a privacy board as contemplated under the HIPAA Privacy Rule shall satisfy this definition so long as the IRB or privacy board meets the composition requirements of this provision.

Review boards inject valuable, independent professional review for certain proposed uses of consumer health data. Large and consequential uses of consumer health information will benefit from this independent scrutiny. In an effort to stay consistent and not introduce a host of new terms or requirements, this definition is heavily influenced by similar provisions within HIPAA and its accompanying regulations.

We received comments regarding the composition of privacy review boards. Because the framework is focused on health information, any consumer representative must have experience working on consumer health issues to best protect consumers' rights. The definition also makes it clear that IRBs and privacy boards satisfy this requirement so long as they meet each element within the definition.

8. **Publicly Available Information** - The term "publicly available information" means any information that:
- a. Has been lawfully made available to the general public from federal, state, or local government records;
  - b. Is published in a telephone book or an online directory that is widely available to the general public on an unrestricted basis;
  - c. Is video, audio, or Internet content published in compliance with the host site's terms of use and available to the general public on an unrestricted basis; or
  - d. Is published by a news media organization to the general public on an unrestricted basis.

For the purposes of this definition, information is not restricted solely because there is a login requirement associated with accessing the information or a fee. When a user of a social media service creates or shares information on that service, such information is restricted unless it is freely accessible to anyone using the service.

Like many proposals, this framework recognizes that there is individual and societal value in the free flow of information and that even health data may receive reduced protections when it has legitimately been made public. We have tried to craft this definition to capture truly public information while not being overly broad. We also clarify that traditional sources of news, such as newspapers, whose digital presence may have a login and/or small cost associated with their service, are still considered well within the public sphere.

We received several comments regarding publicly available information. Specifically, to address comments about information that requires a fee for access, we eliminated a specific dollar amount in an effort to account for several services that have varying fee schedules.

9. **Research** - The term “research” means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

This definition is heavily influenced by similar provisions within HIPAA, the Common Rule regarding federal human subjects and their respective regulations. This definition permits public interest research to continue while avoiding a loophole that could be used to justify any type of commercial data research.

## Collection and Processing of Consumer Health Information

### I. Obligations for Participating Entities

Currently, the burden of ensuring sufficient privacy protections around health data disproportionately falls on consumers. This portion of the framework focuses on data collection and use practices that ensure data is used for limited purposes consistent with consumer requests and expectations. We have also included data security provisions.

#### A. Relation to Existing Federal, State, and Municipal Laws and Regulations

To the extent that any participating entity’s collection, disclosure, or use of consumer health information is already governed by federal, state, and municipal laws and regulations, those legal obligations are not affected by this framework.

This section is intended to make clear that framework participants must follow all applicable laws and regulations in addition to offering consumers the higher level of protections included within the framework.

## B. Privacy and Security Protections

A participating entity shall offer the same levels of privacy and security protections and data rights and controls to all consumers, regardless of whether the consumer is paying for services or receiving them for free.

## C. Permissible Collection and Use Practices for Consumer Health Information

A participating entity:

1. Shall not collect, disclose, or use consumer health information for any purpose other than the purpose for which the data was originally collected, disclosed, or used;
2. Shall limit the amount of consumer health information collected, disclosed, or used to only what is necessary to provide the product or feature the consumer has requested; and
3. Shall take reasonable efforts to contractually obligate third parties and service providers with whom it discloses consumer health information to also meet the obligations of this framework.

This section is intended to categorically prohibit secondary uses of health data that do not fall under one of the clearly defined exceptions to this framework. If a participating entity would like to offer a new product or functionality or repurpose data for any reason, it must seek affirmative consent for that new use. In no instance should terms of service serve as justification for secondary uses of data. Data collection and use limits carry through to third parties. Consumers should be protected without having to take additional steps to monitor how their data is being used by third parties.

This section is likely to curb some current behavioral advertising and commercial product development activities that do not avail themselves of one of the other exceptions, such as the use of de-identified data. We understand this approach is more stringent than other voluntary frameworks and legal standards, but we believe health data warrants the protection.

To address comments regarding the obligations section, we have clarified that a covered entity shall take reasonable efforts to contractually obligate third parties and service providers. This approach better aligns the framework with similar privacy protections found in other proposals and industries, and provides participating entities and consumers with greater assurance that the framework's protections carry through to third parties.

#### **D. Consumer Health Information Retention**

A participating entity:

1. Shall maintain consumer health information for a period of time only as long as necessary to carry out the purpose(s) for which the consumer health information was collected; and
2. Shall delete all consumer health information once there is no longer a valid reason to retain it.

There should be clear and reasonable limits on the length of time consumer health information may be maintained by participating entities. Retention limits benefit both consumers and participants. Less data can lessen the impact of breaches and ensure that decisions are not made on stale, old, and incorrect data and produces lower storage and security costs. These limits are consistent with limits in other existing proposals and regulations.

#### **E. Prohibitions on the Use of Consumer Health Information to Harm or Discriminate Against Consumers**

1. A participating entity shall not collect, disclose, or use consumer health information to discriminate against consumers.
2. A participating entity shall not collect, disclose, or use consumer health information when making significant eligibility determinations, including housing, employment, healthcare, and other significant determinations.
3. A participating entity shall not draw inferences from a consumer's refusal to use or cessation of use of a platform, product, app, or digital health tool that could lead to discrimination, stigmatization, harmful profiling, or exploitation.

Consumer health information is inherently sensitive. It should not be collected, disclosed, or used in ways that harm or discriminate against consumers, or limit consumers' access to critical life services or opportunities.

To address comments regarding the use of consumer health information to harm consumers, we have included an additional provision within this section. Specifically, the additional section makes it clear that a consumer's decision to not use or to stop using a specific product or service shall not have any negative or harmful consequences.



## F. Security

1. A participating entity shall establish and implement reasonable information security policies, practices, and procedures for the protection of consumer health information, taking into consideration:
  - a. The nature, scope, and complexity of the activities engaged in by such participating entity;
  - b. The sensitivity of any consumer health information at issue;
  - c. The current state of the art in administrative, technical, and physical safeguards for protecting such information; and
  - d. The cost of implementing such administrative, technical, and physical safeguards.
2. Requirements - The policies, practices, and procedures required in subpart (1) of this section must include the following:
  - a. A written security policy with respect to the collection, retention, and use of such consumer health information;
  - b. The identification of an officer or other individual as the point of contact with responsibility for the management of information security;
  - c. A process for identifying and assessing reasonably foreseeable security vulnerabilities in any systems maintained by such participating entities that contain such consumer health information, which shall include regular monitoring for vulnerabilities and breaches of security of such systems;
  - d. A process for taking action designed to mitigate against vulnerabilities identified in the process required by subparagraph (c)—which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software—or for regularly testing or otherwise monitoring the effectiveness of the existing safeguards;
  - e. A process for determining whether consumer health information is no longer needed and for disposing of consumer health information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such consumer health information permanently unreadable or indecipherable;
  - f. A process for overseeing persons who have access to consumer health information, including through network-connected devices;
  - g. A process for employee training and supervision for implementation of the policies, practices and procedures required by this subsection; and

- h. A written plan or protocol for internal and public response in the event of a breach of security.

This section imposes a “reasonable” security requirement on participants that is consistent with FTC enforcement and the laws in many states. Because “reasonable” is scaled to the sensitivity of the data, the way it is used, and the state of technology, participants’ obligations will be commensurate with the business and engineering decisions they make. The processes required here are also flexible and outcome-based, which is usable for participants of all sizes and sophistication.

## II. Consumer Controls

### A. Consumer Rights With Respect to Consumer Health Information

1. Consumers’ Rights to Access, Correct, and Delete Consumer Health Information:
  - a. A participating entity shall provide a consumer with a free, clear, and easy process for requesting personal consumer health information within the participating entity’s possession.
  - b. A participating entity shall provide a consumer with a free, clear, and easy process for requesting and receiving a list of all other affiliates, service providers, and third parties that have received, licensed, or purchased their consumer health information:
    - i. If a participating entity has shared, licensed, or sold consumer health information to another entity that contracts with one or more individuals who act as independent contractors to provide a benefit (such as transportation, deliveries, or another immediate benefit) directly to a consumer, the participating entity must identify the other entity, but need not list or identify any end-service providers.
  - c. A participating entity shall provide a consumer with a free, clear, and easy process for requesting corrections or deletions to any inaccurate information within the consumer health information in the participating entity’s control.
  - d. A participating entity shall make reasonable efforts to correct or delete a consumer’s health information based on a consumer’s request for correction or deletion.
  - e. When correction or deletion cannot occur, a participating entity shall provide the requesting consumer with an explanation as to why the correction or deletion request cannot be carried out.

To address comments regarding consumers' ability to receive information about all other entities that have received, licensed, or purchased their consumer health information, this section now provides consumers with a clear mechanism to obtain this information. The additions to this section are also necessary because of modifications made to the transparency requirements above that now require that consumers receive information about the types of entities that will receive, license, or purchase their consumer health information. This addition strikes a balance between consumers' interests and the compliance obligations of participating entities.

Additionally, we received comments that raised concerns regarding how information that was at one time HIPAA-covered data (PHI) should be treated under this section. Specifically, commenters raised concerns that a consumer's medical records, records that were once covered by HIPAA and may well be shared in the future with HIPAA-covered entities, should only be annotated and not subject to broader correction and/or deletion requirements. While we recognize these concerns, this framework is designed to operate outside HIPAA and give consumers greater control over their health information. We encourage participating entities that collect, disclose, or use these types of records to ensure that these consumer rights are made clear to everyone via the framework's transparency requirements. Moreover, medical professionals who may receive this type of consumer health information should appreciate that the consumer, and not a HIPAA-covered entity, is deciding what information they are sharing and proceed accordingly.

## 2. Consumers' Portability Rights

- a. Where technically feasible, a participating entity shall make available a reasonable means for a consumer to download their health information that is retained by the participating entity in a structured, standardized, and machine-readable interoperable format for the consumer's own use.

## 3. The Use of Consumer Health Information to Train or Be the Subject of Automated Systems or Processes

- a. A participating entity shall not collect, disclose, or use consumer health information to train or be the subject of any automated, algorithmic, or artificial intelligence (AI) application unless that entity has first:
  - i. Obtained affirmative express consent from a consumer for the use of their health information in such applications, or

- 
- ii. Subjected the consumer health information to be collected, disclosed, or used to a risk-based privacy assessment, any risks identified have been appropriately mitigated, and the use is consistent with a reasonable individual's expectations given the context in which the individual provided or authorized the collection, disclosure, or use of their consumer health information.
  - b. If the consumer health information served as an input for an automated system or process, any resulting data that is produced or results from that automated system or process shall be considered consumer health information if:
    - i. The resulting data relates to or is used to determine, predict, or estimate the past, present, or future physical or mental health condition of an individual;
    - ii. The resulting data relates to the provision of healthcare to an individual; or
    - iii. The resulting data includes:
      - (A) Genetic data;
      - (B) Data that reflects a particular disease or condition;
      - (C) Data that reflects any substance use disorder;
      - (D) Data that reflects reproductive health; or
      - (E) Data that reflects disability.
  - c. Automated, algorithmic, or AI applications, processes and systems must be designed and implemented by the participating entity to mitigate potential algorithmic bias, including through design processes that regularly interrogate the variables and training data used, measures that ensure transparency and explainability, and routine auditing.

We have drafted this section to include several consumer rights that are consistent with existing domestic and international regulations and proposals.

To address comments regarding the use of data sets produced by automated, algorithmic, or AI applications, processes, and systems that used consumer health information in the creation of those subsequent data sets, this section has been modified to align with the framework's definitions to clarify when those new data sets shall be treated as consumer health information.

### III. Notice and Transparency

Section I establishes data collection and use practices that ensure consumer health data is used for limited purposes consistent with consumer requests and expectations. This section builds on those critical protections and is designed to empower consumers with the information they need.

Notice and transparency serve two complementary functions. First, timely and meaningful notice allows individuals to make informed decisions before they agree to have their health information collected, disclosed, or used. Second, ongoing transparency requirements allow individuals to revisit a participating entity's data policies at a time of their convenience or keep up to date with changing data uses. It also allows researchers, regulators, and advocates to track data use trends and better understand companies' practices. Because these purposes require different levels of detail, the framework requires participating entities to prepare two sets of information. This approach provides consumers with the information they need without overwhelming them, while simultaneously providing more thorough information to be used over time or in the public interest.

#### A. Notice

A participating entity shall not collect, disclose, or use consumer health information as permitted under Section I unless it first:

1. Clearly identifies the types of health information that will be collected;
2. Clearly states the purpose(s) that any health information is collected for;
3. Clearly states the data retention policies that will apply to the consumer's health information;
4. States whether any health information will be disclosed and, if so, provides the user clear information about the specific types of entities that will receive, license, or purchase the consumer health information;
5. States the reason(s) any health information is disclosed;
6. Commits to promptly notifying consumers when policies and practices surrounding how their health information will be collected, disclosed, or used have changed; and
7. Provides consumers with a description of their individual rights and a clear list of any consumer controls that a participating entity has made available.

To address comments regarding greater transparency around data retention, this section now contains a provision requiring participating entities to tell consumers how long they will retain the consumers' health information. Retention information can help consumers make informed choices when selecting services and also allow consumers to act should they wish to obtain a copy of their health information before it is no longer retained by an entity.

We also received several comments regarding the framework's notice provisions. Specifically, commenters noted that it may not be possible and/or may be overly burdensome to identify every entity that may receive a consumer's health information at the time they consent to using a product. To address this, the notice provision now requires participating entities to provide information about the types of entities that receive consumers' health information. This modification still permits consumers to make informed decisions when engaging a product for the first time. If a user wishes to know the names of all the entities that may collect, use, or share their information, they may find them in the transparency report required by the next section.

## **B. Transparency**

A participating entity that collects, discloses, or uses consumer health information shall, with respect to each service or product provided by the participating entity, publish:

1. A consumer-facing policy that:
  - a. Includes information regarding each element listed within the "Notice" section of this framework; and
  - b. Is written in a manner that is succinct and easily understandable to a consumer.
2. A complete second and more detailed policy that includes:
  - a. Each element listed within the "Notice" section of this framework;
  - b. The manner in which consumer health information is collected; and
  - c. A detailed list of all affiliates, service providers, and third parties with whom the participating entity has disclosed or plans to disclose consumer health information.

With regard to obligations of a participating entity to list other entities that will receive, license, or purchase consumer health information, if the other entity is one that contracts with one or more individuals who act as independent contractors to provide a benefit (such as transportation, delivery, or another immediate benefit) directly to a consumer, the participating entity must identify the other entity, but need not list or identify any end-service providers.

As a result of the comments we received, this section now includes additional clarity around situations where covered entities work with partners that use independent contractors to provide a benefit. For example, a participating entity need not list the names of individual independent contractor(s) (such as a delivery person); it need only provide the name of the service provider partner.

#### IV. Consent

Participating entities must obtain a consumer's affirmative express consent prior to any collection, disclosure, or use of consumer health information permitted under Section I. Consent adds an important layer of protection and consumer control within the framework by permitting the individual consumer to decide whether or how their health information will be collected, disclosed, or used.

These provisions are drafted to require consumer consent for specific collections and uses of consumer health information, as opposed to a simple blanket consent for a host of possible uses. It also includes important consumer rights to revoke consent later on.

It is important to note that nothing in this section allows "consent" to override any of the categorical prohibitions and obligations in Section I. For example, a person cannot consent to being discriminated against, to having their data used or shared for prohibited secondary purposes, or to being subjected to a pay-for-privacy scheme.

##### A. Elements of Consent

In addition to the obligations for participating entities in Section I, before a participating entity may collect, disclose, or use consumer health information:

1. A participating entity must obtain affirmative express consent from a consumer;
2. A participating entity must seek additional consent for any new collection, disclosure, or use of consumer health information outside the scope of any previous consumer consent;
3. A participating entity may seek to obtain affirmative express consent from a consumer for continued, ongoing, or periodic collection, disclosure or use of consumer health information when both the purpose and intended use of consumer health information is the same for every instance of collection, disclosure, or use; and
4. Affirmative express consent shall be freely given and nonconditioned.

## B. Revocation of Consent

1. A participating entity collecting, disclosing, or using consumer health information must provide consumers with the ability to revoke consent.
2. A participating entity must stop the collection, disclosure, or use of health information once a consumer has revoked consent.

We received numerous comments regarding the framework's consent provision, and recognize that questions around consent and its continued applicability and utility are difficult. While this framework is designed to move beyond existing consent-centric regimes by placing real limits around the collection, disclosure, and use of consumer health information, there are instances where consumers' control of their data matters. Given the sensitivity of the covered health information protected by this framework, consumers must consent before their health data is collected, disclosed, or used.

Additionally, we received comments and questions regarding the frequency of consent required under this section. To address this, we added additional clarifications that make it clear that a single consent is sufficient for continued, ongoing, or periodic collection, disclosure, or use of consumer health information, so long as the purpose and intended use of consumer health information is the same for every instance. Consumers and participating entities should not be overburdened with redundant consent requests.

## V. Exceptions

Nothing in this framework shall limit participating entities from:

1. Engaging in practices that use consumer health information when necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes that adhere to commonly accepted ethical standards and laws:
  - a. With affirmative express consent from a consumer;
  - b. Provided that the research has been reviewed and received written approval by a privacy review board; or
  - c. If the research uses aggregated health data, provided that:
    - i. A participating entity may use aggregated health data for research without consumer consent only after it:



- 
- (A) Determines that the aggregated health data to be used only relates to a group or category of individuals or devices and does not identify and is not linked or reasonably linkable to any individual;
  - (B) Documents the methods and results of the analysis that justify such determination; and
  - (C) Produces a publicly available statement explaining the participating entity's practices regarding the general methods used for aggregating consumer health information;
- d. If the research uses de-identified health data, provided that:
- i. A participating entity may use de-identified health data for research without consumer consent only after it determines that the data is not individually identifiable. This determination shall be made by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, who:
    - (A) Applying such principles and methods, determines that the risk is very small that the de-identified health data could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information;
    - (B) Documents the methods and results of the analysis that justify such determination; and
    - (C) Produces a publicly available statement explaining the participating entity's practices regarding the general methods used for rendering consumer health information not individually identifiable.
2. Engaging in commercial, academic, or research practices that use only publicly available consumer health information.
3. Using or disclosing consumer health information to a medical professional or healthcare provider without consent if that participating entity, in good faith:
- a. Believes that an emergency involving danger of death or serious physical injury to any person requires use or disclosure relating to the emergency; and
  - b. Believes that the recipient of this information is in a position to address, rectify, or prevent the emergency; and
  - c. If a participating entity uses this emergency exception, it shall promptly notify the consumer whose health information was disclosed.

- 
4. Engaging in practices that use consumer health information when necessary and solely for the purposes of:
    - a. Detecting and preventing security incidents, identity theft or fraud, or protecting against malicious or deceptive activity;
    - b. Performing system maintenance, diagnostics, debugging, or error repairs to ensure or update the functionality of a product or service;
    - c. Complying with a federal, state, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; or
    - d. Addressing health misinformation or moderating content or accounts to prevent harm to consumers.
  5. Collecting, disclosing, or using data:
    - a. About an individual in the course of the individual's employment or application for employment (including on a contract or temporary basis), provided that such data is retained or used by the participating entity or the participating entity's service provider solely for purposes necessary for the individual's employment or application for employment;
    - b. That is emergency contact information for an individual who is an employee, contractor, or job applicant of the participating entity, provided that such data is retained or used by the participating entity or the participating entity's service provider solely for the purpose of having an emergency contact for such individual on file; or
    - c. About an individual (or a relative of an individual) who is an employee or former employee of the participating entity for the purpose of administering benefits to which such individual or relative is entitled on the basis of the individual's employment with the participating entity, provided that such data is retained or used by the participating entity or the participating entity's service provider solely for the purpose of administering such benefits.
  6. Engaging in limited commercial product development:
    - a. With affirmative express consent from a consumer for this specific use, provided that it:
      - i. Uses aggregated health data or de-identified health data;
      - ii. Complies with the provisions of the "Prohibitions on the Use of Consumer Health Information to Harm or Discriminate Against Consumers" section of this framework;

- iii. Meets the requirements of the “Notice” and “Transparency” sections of this framework for this specific and limited use; and
- iv. Does not share any consumer health information, de-identified health data, or aggregated health data used in that development with a third party.

The framework should include very limited exceptions that permit the collection, use, and sharing of health data without consent or for secondary purposes. Mindful of how exceptions can undercut the effectiveness of a framework, these provisions borrow from long-standing laws that attempt to balance the equities between individual privacy, societal benefits from the use of this data, and participants’ needs to process data to deliver the service or product requested by an individual.

To address comments regarding the use exceptions for aggregated and de-identified data, modifications were also made to this section to keep terms consistent throughout the framework. Additionally, to address comments regarding employee data, subsection 5 was added to clearly list limited exceptions for the use of employee data. These points reiterate the provisions of the newly added employee data definition so that employers are not overly burdened when using data about their employees for purely administrative functions.

We received several comments regarding how participating entities should handle employee data under the framework. In response, we have included a new exception that is designed to identify limited, specific instances where data may be collected, disclosed, or used outside the framework’s general provisions for the limited employment-related purposes enumerated here. Data about employees that is collected, disclosed, or used for any other purpose falls outside this exception and is subject to the same protections as the covered data of any other person.

Finally, we received several comments surrounding the use of consumer health information for commercial product development. We recognize that consumer health information can help entities develop innovative new products and services. However, these commercial benefits must be properly balanced with consumers’ rights.

In an effort to strike a balance and permit limited commercial use, we have added language designed to promote strong consumer privacy protections when consumer health information will be used by a participating entity solely for commercial purposes. Specifically, to best protect consumer privacy, this section limits commercial development to aggregated and de-identified data. It incorporates the framework’s antidiscrimination and transparency provisions to ensure consumers will not be harmed and will know how their data will be used. Since this is a new exception, we look forward to continuing to work with our partners and the public on this important provision.

---

# Proposed Self-Regulatory Program: Policy Rationale

For any follow-up questions, kindly contact Alice Leiter at eHI ([alice@ehidc.org](mailto:alice@ehidc.org)).

Numerous efforts in recent years have successfully developed comprehensive codes of conduct and terms of service to protect consumer privacy.<sup>3</sup> Rather than duplicate such efforts, we decided to pursue a more formal, tangible, and meaningful accountability structure: a self-regulatory program for non-HIPAA-covered entities that collect, use, and share health data. This proposal would establish a voluntary self-certification program led by an independent, third-party organization. This reduces the potential for bias and lax internal policing, increases the possibility for meaningful adherence to privacy practices, and ensures consequences for nonadherence.

## Addressing Consumer Trust

While we grappled with options to protect consumer privacy, a self-regulatory model arose as the most effective option available in the current environment. Perhaps most relevant to this project, self-regulation can engender trust: "...[T]he most important goal of any self-regulatory system is building consumers' trust in its participants. Self-regulation often arises in response to erosion of trust.... Laws rarely achieve the goal of building trust, because they merely set a baseline for compliance."<sup>4</sup> Further, self-regulatory programs can be nimbler and more flexible than government regulation.<sup>5</sup>

Successful self-regulatory programs can create trusted environments by "setting standards that only responsible organizations can meet. Participants in the self-regulatory system obtain the benefit of differentiating themselves from others whose conduct, while it may be legal, is not exemplary."<sup>6</sup> Moreover, public reporting of compliance with the standards provides a level of transparency and accountability that further engenders trust.

Self-regulation incentivizes competitors to monitor each other for compliance with the agreed-to standards. It provides consumers with a clear and straightforward way to file complaints. Most important, self-regulatory programs are based on a neutral enforcement mechanism.

---

<sup>3</sup> See Manatt White Paper at pp. 16–17. This paper provides an in-depth discussion on self-regulation, what models have been implemented and how they have worked in other industries, and how one might work in healthcare. We have pulled out key points for this policy rationale but encourage a full read of the paper for a more thorough look at the benefits and particulars of a self-regulatory model for non-HIPAA-covered entities.

<sup>4</sup> Boulding, M. "Self-Regulation: Who Needs It?," *Health Affairs*, Volume 19, Number 6 (2000), available at <https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.19.6.132>.

<sup>5</sup> See Manatt White Paper at pp. 17–27.

<sup>6</sup> Boulding, M. "Self-Regulation: Who Needs It?," *Health Affairs*, Volume 19, Number 6 (2000), available at <https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.19.6.132>.

## Program Goals

The goal of the program envisioned by our framework is that compliance with the self-regulatory program would be viewed by consumers as a “Good Housekeeping Seal of Approval,” i.e., the gold standard for privacy-protecting technology. Through widespread promotion and adoption, certification of technology products through the program would ultimately become the industry standard.

Key tenets of the proposal are strong accountability and enforcement mechanisms, including comprehensive audits, spot checks and annual assessments, all of which would complement existing government regulation through the FTC.<sup>7</sup> The program would act as a partner to FTC regulators and state attorneys general (AGs) in that it would offer its participants compliance resources that government authorities may not have, such as time, infrastructure, and industry expertise.<sup>8</sup> This program would offer widespread monitoring and, given the already stretched resources of the FTC in particular, allow the commission to focus its efforts against the most egregious violators.

## Establishment of a New Self-Regulatory Program

Operationalizing a new self-regulatory program will take extensive planning. Discussions about who might house a program of this type have centered around how the program should function rather than who should manage it. Although no final recommendations about program ownership were determined, several related issues were identified as needing further exploration. These will be considered during the second phase of this work:

- Ideally, the program would be housed in an existing organization rather than stood up as a brand-new entity. Succeeding at the latter would require more resources and a significantly heavier lift in terms of establishing name recognition and figuring out program logistics and a management structure. A number of reputable organizations have experience running self-regulatory programs in other industries.
- An organization that has a road map in place with experienced personnel to implement the new program would also lend credibility to the entire program for both consumers and regulators. There may be a need for an advisory body as part of the governance structure, another area for determination at a later date.
- A funding mechanism. Although funding details are for a later phase of work, the intention is that participating entities would pay an annual fee, scaled based on their size in terms of gross revenue.
- A sound economic model is key to a successful program, and in the implementation phase of this work, significant time and attention would be devoted to related logistics and ensuring that there are no conflicts of interest, whether real or perceived.

<sup>7</sup> While the Office for Civil Rights within the Department of Health & Human Services is the compliance and enforcement body for HIPAA-covered entities, it is the FTC that has similar authority for businesses outside HIPAA, even if they collect and use health data.

<sup>8</sup> See Manatt White Paper at p. 22.

## Consumer and Participant Benefits

An inherent tension exists between “carrots” and “sticks” for encouraging and driving participation in the proposed program. Shoring up protections for consumers, as well as providing accountability and enforcement mechanisms, were the key areas this proposal sought to address. Consumers are often skeptical of self-regulation in the healthcare space due to perceived bias among participating companies. The introduction of a third-party, independent monitoring entity, with the backstop of FTC enforcement, would help assuage those worries.

During the next phase of this work, we will devote significant time and effort to involving consumers and consumer advocacy groups in fleshing out how this program will be implemented. Addressing consumer skepticism head-on by engaging consumer groups in these discussions will be critical.

To ensure the success of this program, participating entities will need meaningful incentives to join. The program will provide participants a way to distinguish themselves in an increasingly competitive market marked by widespread consumer distrust. And this benefit is real: [Cisco’s 2020 Data Privacy Benchmark Study](#), drawing from data from 2,800 organizations in 13 countries, showed that 70 percent of organizations say they received significant business benefits from privacy beyond compliance—up from 40 percent in 2019.<sup>9</sup> Further, “82 percent of organizations see privacy certifications as a buying factor: Privacy certifications ... are becoming an important buying factor when selecting a third-party vendor.”<sup>10</sup>

As noted in the Executive Summary above, this framework creates a potential road map for future data privacy legislation. Companies that join as participants thus have the potential to be “ahead of the curve” when adopting the framework’s policies. The combination of this with reputational and commercial benefits should provide significant incentives for companies to join.

## Incorporation of Feedback

We received a number of thoughtful and detailed comments from a variety of stakeholders on all aspects of this framework, including the proposed self-regulatory structure. The above strives to address the majority of these, as do the adjustments to the following proposal. The most significant change to the draft released in August is the explicit recommendation that this new program be housed in an existing entity rather than established as a brand-new, stand-alone organization. As articulated above, we believe this will put us in a much stronger position for eventual implementation as well as help address many of the logistical and reputational questions we received. Perhaps most important, a reputable umbrella organization would help our program achieve far greater stakeholder confidence and trust, ultimately making it more meaningful for consumers and more attractive to potential participants.

---

<sup>9</sup> “Cisco 2020 Data Privacy Benchmark Study Confirms Positive Financial Benefits of Strong Corporate Data Privacy Practices,” available at [https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2047256&utm\\_source=newsroom.cisco.com&utm\\_campaign=Release\\_2047256&utm\\_medium=RSS](https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2047256&utm_source=newsroom.cisco.com&utm_campaign=Release_2047256&utm_medium=RSS).

<sup>10</sup> *Id.*

# Self-Regulatory Program for Non-HIPAA Healthcare Data

The proposed framework structure is a self-regulatory program focused on accountability: an independent, self-certification model designed to hold participating entities to a set of standards separately developed through a multistakeholder process. The program, housed in and run by an independent nonprofit organization, would accept individual companies as participants. Participating entities would submit their products for certification and individual products validated as compliant with the framework would be certified.<sup>11</sup>

Participating entities would undergo a thorough onboarding review at enrollment, be educated as to the self-regulatory framework and its obligations, publicly commit to complying with it, and submit to annual audits and assessments. Additionally, active spot-check monitoring would be done on a random sample of participants throughout each year. Participating entities could publicly market their participation and certification level as an “XXX Health Data Privacy Participant” (name TBD) and receive a recognizable visual certification symbol to mark them as such.

Participant fees would be collected from participating organizations to maintain the program. The amount of the fee would be on a sliding scale, based on the size of the company in terms of gross sales. Annual fees would also depend on the amount of seed money put forward to stand up the program at its origination.

Relevant components of this program would include:

- Rigorous onboarding, including the submission of a detailed questionnaire regarding business practices to ensure compliance with program standards;
- Annual audits and compliance assessments;
- Ongoing monitoring of participant companies, including random spot checks;
- Criteria to ensure that the reviews and assessments conducted by the program are independent of the program’s administrative and financial functions;
- A public commitment by each company to follow the program’s standards;
- Maintenance by the program of a dedicated, public-facing website describing the program’s goals, requirements, and governance logistics; listing participating covered organizations; and providing a simple and straightforward method for consumers to ask questions and file complaints about any product and/or any participating covered organization;

---

<sup>11</sup> Included entities will be all companies that collect, use or process health-related personal data. These would include, among others: hardware manufacturers; app developers; website publishers; third-party data management, brokering, collection or use outfits; and, potentially, businesses/employers that rely on third-party health technology in order to maintain the health of their workers.



- A standardized set of privacy rules that includes:
  - A broad, use-based definition of consumer health information;
  - Articulated appropriate uses and obligations surrounding the collection and use of consumer health information;
  - Greater consumer access to and control of their health information; and
  - Clear notice and transparency requirements; and
- An annual report card by program staff, publicly released, detailing the program’s activities and effectiveness during the preceding year in obtaining compliance by participating covered organizations and in taking meaningful disciplinary and corrective actions for noncompliance.

Accountability and potential enforcement mechanisms for participating entities would include:

- Independent monitoring by program staff or other authorized evaluators, including publicly announced corrective or disciplinary cases;
- An active complaint-gathering process, clearly articulated in all public-facing materials and websites;
- A dispute resolution mechanism for resolving consumer complaints or complaints by another company based on the program’s standards, and potentially providing consumers with redress for violations;
- A requirement to develop a corrective action plan (CAP) in the event of noncompliance and a process to lose certification if the CAP fails;
- Public announcement of investigations into complaints and complaint resolution, ensuring no complaints are ignored;
- Penalties for persistent or willful noncompliance with the law and the program’s standards, such as suspension or dismissal from the program and/or referral to the FTC and/or state AG; and
- Potential for FTC and/or state AG enforcement of violations of agreed-to standards.

This type of self-certification program would help level the playing field among businesses, fostering a unified set of privacy practices that are responsive to recent regulation. At the same time, it would raise the bar for consumer privacy in an area of great personal sensitivity.

The critical difference between this program and a more passive, pledge-style or “best practices” program is the inclusion of rigorous onboarding and ongoing accountability assessments, all of which are designed to elicit full compliance from well-intentioned actors and prevent bad actors from falsely shielding their inappropriate conduct behind a pledge. Significantly, such a program could easily be converted into a safe harbor-style accountability mechanism in future legislation, giving it lasting utility even should new laws be passed.



# Appendix

## Steering Committee Members

The following organizations and individuals are some of those who participated in the development of this framework by virtue of being part of our Steering Committee. This committee met twice, in February and July of 2020, and many members also participated in one of our workgroups and/or offered feedback on earlier drafts of these proposals. Participation in the Steering Committee does not signify an endorsement of this framework, either in whole or in part. Rather, our Steering Committee provided valuable counsel and constructive criticism over the course of the framework's development. This final product reflects the work of the Center for Democracy & Technology and the eHealth Initiative alone.

**Joseph Ashkouti**  
Change Healthcare

**Jacqueline Baratian**  
Ascension Health

**Julie Barnes**  
Maverick Health Policy

**Robert Belfort**  
Manatt

**William Bernstein**  
Manatt

**Melissa Bianchi**  
Hogan Lovells

**Susan Bouregy**  
Yale University

**David Brody**  
Lawyers' Committee for  
Civil Rights Under Law

**Rebecca Cady**  
Children's National Hospital

**Shawneequa Callier**  
George Washington  
University

**Joanne Charles**  
Microsoft

**Henry Claypool**  
American Association of  
People with Disabilities  
Consultant

**Andy Coravos**  
Elektra Labs

**Corey Cutter**  
American Cancer Society

**Paul Eddy**  
Wellmark

**Mary Engle**  
BBB National Programs

**Shari Erickson**  
American College of  
Physicians

**Dani Gillespie**  
National Partnership for  
Women & Families

**Tina Grande**  
Healthcare Leadership  
Council

**Carlos Gutierrez**  
LGBT Technology  
Partnership & Institute

**Rachele Hendricks-  
Sturup**  
Future of Privacy Forum

**Laura Hoffman**  
American Medical  
Association

**Alice Jacobs, M.D.**  
Convergence Group

**Sean Kennedy**  
Salesforce

**Jeri Koester**  
Marshfield Clinic  
Health System

**Erin Mackay**  
National Partnership for  
Women & Families

**Amy McDonough**  
Fitbit

**Meg McElroy**  
Ascension Health

**Deven McGraw**  
Citizen

**Dena Mendelsohn**  
Elektra Labs

**Ben Moscovitch**  
The Pew Charitable Trusts

**Brenda Pawlak**  
Manatt

**Jules Polonetsky**  
Future of Privacy Forum

**Jessica Rich**  
Institute for Technology Law  
and Policy at Georgetown  
University Law Center

**Alejandro Roark**  
Hispanic Technology  
& Telecommunications  
Partnership

**Rajeev Ronanki**  
Anthem, Inc.

**Alaap Shaw**  
Epstein Becker Green

**Ashley Thompson**  
American Hospital  
Association

**Lee Tien**  
Electronic Frontier  
Foundation

**Charlotte Tschider**  
Loyola University Chicago  
School of Law

**Nicol Turner-Lee**  
Brookings Institution

**Ann Waldo**  
Waldo Law Offices

**Marcy Wilder**  
Hogan Lovells

**Po Yi**  
Manatt

**Ashwini Zenooz**  
Salesforce

FOR MORE INFORMATION, PLEASE CONTACT:

---

**Center for Democracy  
& Technology**  
CDT.ORG

**Andrew Crawford**  
Policy Counsel  
acrawford@cdt.org

**eHealth Initiative  
& Foundation**  
EHIDC.ORG

**Alice B. Leiter**  
Vice President and Senior Counsel  
alice@ehidc.org

© 2021





February 8, 2020

### **Privacy and Security Round Up**

#### **OCR's \$4.3 Million Penalty against MD Anderson Cancer Center Overturned**

On January 14, 2021, the Fifth Circuit [vacated](#) a \$4,348,000 penalty that the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) had imposed on the University of Texas M.D. Anderson Cancer Center (MD Anderson) for alleged violations of the HIPAA Privacy and Security Rules in 2012 and 2013. The fines arose from the loss of two thumb drives and a stolen laptop holding unencrypted protected health information (PHI) of nearly 35,000 individuals. The court vacated the penalty on four grounds: (1) HHS had failed to show that MD Anderson did not implement an "encryption mechanism" simply because 3 workforce members failed to use it to encrypt PHI; (2) the passive loss of information is not an "disclosure," which requires both an affirmative act and and to someone outside the entity; (3) the fine was far higher than fines imposed on other covered entities in comparable situations; and (4) in calculating the fine, OCR exceeded the statutory maximum annual penalty of \$100,000 per "reasonable cause" violation.

*Comments: The decision represents a stinging rebuke by the Fifth Circuit of OCR's interpretation of the HITECH Act, OCR's own regulations, and its enforcement process. Since OCR had already lowered the maximum penalties in a [Notice of Enforcement Discretion](#) issued in April 2019 (possibly in response to the MD Anderson challenge), the impact of this decision will likely be with respect to the other three grounds for vacating the penalty. Of particular interest are the Court's determinations that: (1) all that the HIPAA Security Rule requires with respect to an encryption mechanism is that the entity have such a mechanism, and that the Rule "says nothing about how effective" the mechanism must be; and (2) when data is lost or stolen, this is not necessarily a "disclosure" as defined in the HIPAA Privacy Rule. In light of this decision, it would not be surprising if OCR proposed amendments to the HIPAA Privacy and Security Rules to address these two determinations.*

#### **HITECH Act Amendment Requires HHS to Consider Recognized Security Practices in Taking Compliance Actions**

On Jan. 5, 2021, the President signed into law [H.R. 7898](#) that amends the HITECH Act to requires HHS to consider, in deciding whether to reduce fines, terminate audits early, or agree to more favorable settlement terms, whether a HIPAA entity had in place "recognized security practices" for at least the prior 12 months. "Recognized security practices" are defined as standards or practices developed under the National Institute of Standards and Technology (NIST) Act, the Cybersecurity Act of 2015, and other regulatory or statutory authorities to address cybersecurity. The new laws states that HHS may not increase penalties or lengthen audits if an entity has not implemented these security practices, but at the same time the new law does not limit HHS's authority to enforce the HIPAA Security Rule or supersede a covered entity or business associate's obligations under the HIPAA Security Rule.

*Comments: The new law is clearly intended to encourage the adoption of "recognized security practices" by HIPAA entities, but it is important to note that it does not establish a safe harbor against HIPAA liability for those entities that implement such practices. In addition, there is currently nothing to prevent HHS from taking into account the security practices implemented by an entity in determining the severity of its enforcement action, and one would expect HHS to do so. Nevertheless, the law is helpful in allowing HHS to focus primarily on an entity's security measures, rather than the fact that it suffered a data breach, in determining appropriate enforcement action.*

#### **FCC Finalizes Restrictions on TCPA Exemptions and Separately Allows Clinical Trial Calls**

On December 30, 2020, the Federal Communication Commission (FCC) issued an [Order](#) finalizing new restrictions on certain Telephone Consumer Protection (Act) exemptions, including the exemption for calls by HIPAA entities to residential lines using an artificial or prerecorded voice. The FCC Order limits the number of such calls to one per day up to a maximum of three such calls per week. It also requires that called parties be permitted to opt out of future calls

using one of two methods specified in the Order. The FCC dismissed concerns that such limits would interfere with the ability of health care providers to communicate with their patients, noting that the same limit already applies for exempted HIPAA calls to wireless numbers.

In a separate [Order](#) issued on January 15, 2021, the FCC confirmed that an artificial or prerecorded voice message call to a residential telephone line seeking a consumer's participation in a clinical trial, but that does not include any advertising or telemarketing, is exempt from the TCPA's prior-express-written-consent requirement. Consistent with its December 30, 2020 Order, the calls must be limited to no more than three within any consecutive 30-day period, and the called party must be allowed to opt out of future calls.

*Comments: While not unexpected, it is disappointing that the FCC decided to impose limits and opt-out requirements for calls made under the HIPAA exemption, particularly in light of the fact that most commenters appear to have opposed these limitations. By contrast, the Order confirming that calls inviting consumers to participate in clinical trials are not considered telemarketing will provide welcome certainty to clinical trial organizations, and is consistent with OCR's position that such communications do not constitute marketing under HIPAA.*

### **FTC Announce Proposed Settlement with Health App Developer Flo For Misrepresenting its Privacy Practices**

On January 13, 2021, the Federal Trade Commission announced a [proposed settlement](#) with the developer of Flo, a period and fertility health app, for sharing the health information of its users with "dozens" of data analytics providers, including Google and Facebook, in violation of its stated privacy practices. Flo allowed the third parties to use the data for their own purposes, despite repeated statement in Flo's privacy policy that it shared only limited data with third parties, and even then, only as necessary to provide its services. Among other things, Flo will be required to provide a notice of the settlement with users, ask the third parties to destroy the information they received, and obtain users' affirmative express consent to share their personal health information with third parties in the future.

*Comments: It is notable that two Democratic Commissioners [partially dissented](#), arguing that the FTC should have charged Flo with violating the Health Breach Notification Rule applicable to non-HIPAA personal health record vendors. They also expressed the desire for "substantive limits on firms' ability to collect and monetize our personal information" and "more authority from Congress in the privacy space." This echoes the view of many, but it remains to be seen whether the new Congress will be able to accomplish this.*

### **OCR Announces Enforcement Discretion for Use of Online or Web-Based Apps for COVID -19 Vaccine Appointments**

On January 19, 2021, OCR issued a [Notice of Enforcement Discretion](#) announcing that it will not impose penalties for HIPAA violations by health care providers or their business associates who in good faith use non-public facing online or web-based scheduling applications (WBSAs) for scheduling COVID-19 vaccination appointments during the public health emergency. The enforcement discretion also extends to WBSA vendors that may not be aware of the use of their apps for this purpose and therefore, that they are business associates. The Notice encourages the use of reasonable safeguards to protect the data, such as using only the minimum necessary data, encryption technology, enabling all available privacy settings and ensuring that the app stores the data only temporarily.

*Comments: While the Notice does not mandate the use of reasonable safeguards, it does state that the lack of reasonable security safeguards will be viewed as a lack of good faith. Nevertheless, and despite its narrow scope, this enforcement discretion provides important protection for affected health care providers.*



**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.**

# Does your health app protect your sensitive info?

[January 13, 2021](#)

by Miles Plant

Attorney, Division of Privacy & Identity Protection, FTC

New health apps are popping up every day, promising to help you track your health conditions, count your calories, manage your medications, or predict your ovulation. These apps often ask for some of your most sensitive personal information, like your health history, medication list, or whether you have ever suffered a miscarriage.

Some apps use that sensitive information only to give you services. But others may use it for their own research, to target you with ads, or disclose — or even sell — your data to other companies. And, unlike your doctor, these apps may not be covered by health privacy laws like HIPAA.

For example, Flo is a health app that functions as an ovulation calendar, period tracker, and pregnancy guide. In a settlement announced today, the [FTC said that the makers of the Flo app](#) shared users' personal health information with marketing and analytics companies like Facebook and Google — even though it had promised users to keep this sensitive information private. As part of the settlement, Flo Health, Inc. has agreed to get users' consent before it can share their information in the future. The settlement also requires Flo to get an outside review of the honesty of its privacy promises.

How can you avoid the risks associated with these types of health apps? Here are some things to consider:

- **Compare privacy protections.** Many competing health apps offer similar services. When choosing between apps, compare their privacy protections. Look for a privacy notice that explains in simple terms what health information the app collects from you, as well as how it uses and shares your information with other companies and users. If the app shares your information, does it tell you why, and does it limit what others can do with it?
- **Take control of your sensitive information.** Take a look at the app's settings to see if it gives you control over what health information it collects and shares. An app's default settings often encourage sharing, so it can be useful to select more protective options.
- **Keep your app up to date.** App updates sometimes include important fixes for privacy or security glitches. One of the best ways to protect your information is to keep your app (and your phone's operating system) up to date.
- **Recognize the risks.** What sensitive information will the app have access to? Are the app's services worth the risk of someone else getting hold of that? Some companies don't uphold their privacy promises. In this case, we said that even if you reviewed Flo's privacy promises and looked at the settings, your information could still have been disclosed to other companies. Sharing sensitive information always carries risks, so be sure you're comfortable with what you've shared, in case privacy promises aren't kept.

- **Report your concerns.** If you think a health app isn't keeping up its end of the bargain, [let the FTC know](#). The FTC regularly brings enforcement actions against companies that misrepresent how they use or disclose people's sensitive health information.



# Using a health app?

Here are some ways to **protect your privacy** and reduce the chance of identity theft and other fraud.



## Compare options on privacy.

When you're considering a health app, ask some key questions.

- Why does the app collect your information?
- How does the app share your information — and with whom?
- Then, choose the app with the level of privacy you prefer.



## Take control of your information.

Do app settings let you control the health information the app collects and shares?

And is your app up to date?



## Know the risks.

Are the app's services worth risking your personal information getting into the wrong hands?



FEDERAL TRADE  
COMMISSION



## Report your concerns.

Do you think a health app shared personal information without your permission?

Tell the FTC at  
[ReportFraud.ftc.gov](https://www.ftc.gov/identitytheft)



## Report identity theft.

Do you think your identity was stolen as a result of using a health app?

Report it at  
[Identitytheft.gov](https://www.ftc.gov/identitytheft).

Blog Topics:

[Privacy, Identity & Online Security](#)



# AI and Healthcare



This POSTnote gives an overview of AI in the healthcare system and its potential impacts on the cost and quality of healthcare, and on the workforce. It summarises the challenges to wider adoption of AI in healthcare, including those relating to safety, privacy, data-sharing, trust, accountability and health inequalities. It also outlines some of the regulations relevant to AI and how these may change.

## Background

There is no universally agreed definition of AI, but it typically refers to systems that can perform tasks that usually require human intelligence.<sup>1</sup> AI systems are underpinned by algorithms; computerised instructions used to perform tasks (such as suggesting a certain diagnosis from a set of symptoms).<sup>2</sup> There are numerous applications of AI across healthcare, including improving diagnostics, monitoring patient health using apps and wearables, and automating administrative tasks.<sup>1-5</sup> Currently, AI is not used widely within the NHS, though some local trials are taking place. For example, the East Midlands Imaging Network and partners are testing AI tools to analyse mammograms for signs of breast cancer and manage screening resources.<sup>6-9</sup>

In the 2017 Industrial Strategy the UK Government stated its aim to use data and AI to “transform the prevention, early diagnosis and treatment of chronic diseases by 2030.”<sup>10,11</sup> In 2018, it invested £50m in five new centres of excellence for using AI to improve diagnostic imaging and pathology,<sup>12</sup> with a further £50m allocated as part of its long-term response to the COVID-19 pandemic.<sup>13</sup> In 2018, the Government published its code of conduct for data-driven health and care technology, aiming to promote best practice among those developing and using AI.<sup>14</sup> Improved use of AI and digital healthcare technologies is identified as a priority in the 2019 NHS Long Term Plan.<sup>15</sup> The 2019 Topol Review set out the new skills which would be required of the NHS workforce to implement these technologies successfully.<sup>16</sup>

## Overview

- Artificial Intelligence (AI) can be used for tasks such as helping clinicians make decisions and monitoring patient health.
- AI systems could lead to improved health outcomes, but few have been trialled and evaluated in real-world clinical settings.
- Automation may reduce the time spent by staff on routine work, though they may require new skills to use AI systems.
- There are some public concerns AI could dehumanise healthcare, though others argue staff time saved through automation could then be spent caring for patients.
- Patient data are often used to produce and test AI systems, raising issues around data quality, accessibility and patient privacy.

In 2019, the Government established NHSX, a new unit responsible for setting policy and best practice around the use of digital technologies in England.<sup>17</sup> This included the creation of an AI Lab with £250m of funding to support the development and deployment of AI technologies in the NHS and care system.<sup>18</sup> The NHS AI Lab’s activities include the AI in Health and Care Award, awarding £140m of funding to support the testing and evaluation of promising AI technologies.<sup>19,20</sup>

## Healthcare AI technology

Some clinical software has incorporated AI since the 1970s, but these systems typically use algorithms with a large set of pre-programmed rules.<sup>21</sup> Advances in AI have been made using machine learning (ML) algorithms (Box 1), which allow systems to learn from example data (known as ‘training data’).<sup>22</sup> ML capability has improved in recent years due to increasing computing power, greater availability of training data, and development of more sophisticated algorithms using techniques like deep learning (Box 1).<sup>22</sup> Healthcare AI systems are being developed in academia and industry, often in partnership with healthcare providers and professionals.

## Data and development

Large, good-quality datasets are needed to train and test AI systems, and may be taken from various sources depending on the intended use. Some systems, such as those used for treatment recommendation and drug discovery, use chemical databases or public clinical literature.<sup>23,24</sup> In other cases,



developers use data from individuals. They may use data from healthcare providers, such as Electronic Health Records (EHRs) ([POSTnote 519](#)) or medical images.<sup>1,5</sup> In some cases, they may collect data directly using apps or wearable sensors.<sup>25–27</sup>

Developers obtain patient data through data sharing agreements. These may be made with NHS trusts, other healthcare providers, or holders of regional or national datasets.<sup>28</sup> Such datasets include data volunteered by patients to studies like the UK Biobank,<sup>29–32</sup> and data gathered from healthcare providers by NHS Digital (which provides data and IT services for health and care organisations in England).<sup>33–35</sup>

## Applications of AI

Commercial AI systems are already used in some NHS settings.<sup>36</sup> However, most AI products for healthcare are still at the research or development stage,<sup>37</sup> with a few at various stages of trial and evaluation in NHS settings.<sup>38–40</sup> This section outlines some of the applications of AI in healthcare settings. It does not cover the use of AI in medical research.

### Medical imaging

There is a large amount of development activity in medical imaging, due to widespread use of standard image formats that provide suitable datasets to train AI systems on and recent improvements to image recognition from deep learning (DL, Box 1).<sup>37,41</sup> DL has the potential to offer faster and more accurate interpretation of medical images.<sup>42–46</sup> Research has shown DL can be used across various specialties, including:

- **Radiology.** AI systems can be used to detect bone fractures and tumours in X-ray images.<sup>8,47–50</sup> Head CT scans can be analysed to detect and characterise strokes,<sup>51–53</sup> traumatic brain injuries and dementia.<sup>54,55</sup>
- **Pathology and endoscopy.** Benign and malignant tumours can be distinguished by analysing microscopic images of tissue samples.<sup>56,57</sup> Cancerous and pre-cancerous polyps can be highlighted in real-time colonoscopy videos.<sup>58,59</sup>
- **Ophthalmology.** Diseases such as glaucoma, diabetic retinopathy and age-related macular degeneration can be diagnosed and monitored using retinal photographs.<sup>60–62</sup>

### Logistics and administration

Administrative and clinical staff spend a significant amount of time on operational tasks, with surveys indicating some staff believe this detracts from clinical work.<sup>63–65</sup> AI has the potential to automate some of these tasks. For example, speech processing techniques can be used to transcribe patient notes.<sup>66,67</sup> Patients who are likely to miss appointments can be automatically predicted and sent reminder messages.<sup>68,69</sup> AI can also be applied to complex logistical problems, such as managing resources and schedules.<sup>70–77</sup>

### Treatment planning and patient monitoring

Decision support systems are software-based AI tools that can support clinicians with tasks, including prescribing drugs,<sup>78</sup> diagnosing conditions,<sup>79,80</sup> and identifying patients at risk of adverse events.<sup>81,82</sup> Systems using pre-programmed rules based on clinical knowledge or guidelines originated in the 1970s,<sup>21,83</sup> and are widely used.<sup>83</sup> Current research on ML-based systems aims to improve performance by learning rules from patient data or clinical literature.<sup>24,84–88</sup> AI systems can also directly

monitor patient health. In hospital, systems using cameras and wearable sensors to provide early warnings of adverse events; such as pressure ulcers,<sup>89</sup> delirium,<sup>90</sup> or circulatory failure;<sup>91</sup> have been researched. High-risk patients outside hospitals can be remotely monitored for deterioration, to avoid unnecessary hospital admissions.<sup>92</sup>

#### Box 1: Machine Learning

A machine learning (ML) algorithm learns to perform a task by coming up with a set of rules to describe patterns in training data.<sup>93</sup> It then applies the rules it has learnt to unfamiliar data. Generally, the more data used to train a ML system, the more accurately it can match true patterns in the data it is applied to.<sup>94</sup> There are two main types of ML algorithm used in healthcare:<sup>93,95</sup> Supervised algorithms learn pre-existing categories in data (such as learning from labelled X-ray images, then detecting tumours in new images).<sup>47–49</sup> Unsupervised algorithms identify categories in data by themselves (for example, finding groups of patients with similar symptoms to help identify common causes).<sup>96</sup>

#### Deep Learning

Many recent advances in ML can be attributed to deep learning (DL), which is a type of ML design inspired by the way neurons transmit information in the brain.<sup>41,93</sup> Deep learning methods have driven improvements in areas such as image and speech recognition ([POSTnote 633](#)).<sup>22,41</sup>

### Patient-facing applications

Some voice assistants and text-based chatbots can be used directly by patients to check symptoms or access treatment.<sup>97–102</sup> Smartphone apps, sometimes with wearable sensors and other devices, can help patients to self-manage conditions like respiratory illnesses,<sup>103–106</sup> diabetes,<sup>107,108</sup> or epilepsy.<sup>109</sup> AI can be embedded in these systems to help to track a patient's condition and offer tailored guidance. Similar systems can be used by patients to self-administer electrocardiography (ECGs)<sup>38,110,111</sup> and urine tests.<sup>112</sup>

### Impact on healthcare

#### Cost of healthcare

Automation of administrative and clinical tasks with AI could cut costs and increase productivity.<sup>113,114</sup> Estimated cost savings vary, but a 2018 report by the Institute for Public Policy Research estimated that AI and automation could save the NHS £12.5 billion per year by freeing up staff time.<sup>115</sup> Some studies have reported AI systems that can equal or outperform clinicians at certain diagnostic tasks, for example in the diagnosis of skin cancer and diabetic retinopathy.<sup>45,46</sup> This could mean diseases are diagnosed earlier or more accurately, reducing future treatment costs.<sup>5,11</sup> However, some researchers have raised concerns around studies of AI performance, noting that few compare performance in real-world clinical settings.<sup>116–119</sup> New reporting standards for evaluation studies have been developed to address this issue.<sup>120–125</sup>

#### Patients

Earlier or more accurate diagnosis of an illness could allow patients to access treatment before complications develop, improving health outcomes.<sup>5,11</sup> There is also evidence of some home monitoring apps enabling patients to engage more with their treatment plans, improving self-management of long-term conditions.<sup>126,127</sup> Some stakeholders have raised concerns that

the use of AI risks dehumanising the healthcare system.<sup>128</sup> Studies of public opinion have suggested people believe human empathy is an important part of healthcare, and that it is important AI systems do not erode the patient-doctor relationship. Some feel that doctors are able to make more holistic judgements about diagnoses or treatments than AI systems.<sup>129–131</sup> Other stakeholders have suggested automation of routine work would allow staff to spend more time with patients, and AI could enable more personalised care.<sup>3,16,132</sup>

### **Healthcare workforce**

Healthcare staff may require new skills and training. For example, they will need the technical knowledge to operate and understand the limitations of AI systems.<sup>16,133</sup> Improved skills in data collection and curation would assist in the development and evaluation of AI systems.<sup>16</sup> New technology-focused roles may be created, such as roles focused on data engineering or governance.<sup>134</sup> PwC predicts a 22% increase in UK healthcare jobs in the period 2018–2028, as the use of AI increases.<sup>135</sup> Health Education England (HEE), which coordinates the training of healthcare workers in England, has established programmes to educate healthcare leaders and clinicians on digital technologies. These include the NHS Digital Academy,<sup>136,137</sup> and the Topol Programme for Digital Fellowships.<sup>138</sup> Some bodies are aiming to professionalise the workforce that develop and use IT and data-driven technologies.<sup>139–141</sup> The Faculty of Clinical Informatics and Federation for Informatics Professionals are working to do this in the healthcare sector.

### **Ethical, social and legal challenges**

In 2020, consultancy company Oxford Insights ranked the UK's overall readiness for AI as second best in the world, behind the US.<sup>142</sup> However, some stakeholders have highlighted long-standing difficulties scaling up innovations in the NHS, citing problems such as a lack of dedicated funds and fragmented organisation of services.<sup>143–146</sup> A number of technical and ethical issues are also associated with AI implementation.

### **Safety and efficacy**

While AI systems have the potential to improve patient outcomes,<sup>147</sup> they may also present significant safety risks if they are poorly designed or do not work as intended.<sup>4,148,149</sup> An AI system may give dangerous recommendations in situations that its programming does not expect, or which were not included in its training data.<sup>150</sup> For example, there have been reports of some chatbot apps missing simulated signs of heart attacks and child sexual abuse during testing.<sup>151,152</sup> If a system is programmed to be overly sensitive, it may over-diagnose patients, leading to unnecessary and risky clinical interventions and increased healthcare costs.<sup>153,154</sup>

Even if an AI system is shown to perform well during development, there may be challenges to its implementation that reduce its effectiveness.<sup>133</sup> For example, a Google retinal disease detection system was found to behave poorly when deployed in several hospitals in Thailand, despite performing as accurately as a human specialist during development.<sup>46,155–157</sup> This was because retinal scans taken in practice were of worse quality than those on which it had been trained. There are also issues around human interaction with AI systems. Health

professionals' cognitive biases can cause them to place undue trust or distrust in an automated decision.<sup>150,158</sup>

NHSX and the National Institute for Health and Care Excellence (NICE), in collaboration with other stakeholders, have each published assessment criteria for digital health technologies.<sup>159–162</sup> These set out the evidence of safety, clinical efficacy, usability and cost-effectiveness that healthcare providers should seek from a developer before purchasing an AI system.

#### **Box 2: Governance of patient data**

Research use of patient data is subject to several laws and codes of practice. Under the EU General Data Protection Regulation (GDPR)<sup>163</sup> and the Data Protection Act 2018,<sup>164</sup> there must be a lawful basis for use of personal data, such as a patient giving their explicit consent, or more usually provisions for research, medical or public health purposes.<sup>163</sup> Under Common Law, patients must consent to any use of confidential patient data.<sup>165</sup> Researchers can apply to the Health Research Authority to set this condition aside in England and Wales, with other arrangements in Scotland and Northern Ireland.<sup>166–168</sup> There are legal exemptions available for use of such data in public health emergencies.<sup>169</sup> Patients in England can prevent such data being used for purposes outside their individual care, under a national opt-out mechanism.<sup>170</sup>

#### **Anonymisation**

Under the GDPR and guidance such as the Caldicott Principles, researchers are expected to mitigate risks to privacy by using the minimum confidential personal data necessary to accomplish a given task.<sup>163,171</sup> They may do this by removing certain identifying information.<sup>172,173</sup> Data that have had such information removed may still be classed as personal data under GDPR. Fully anonymising data so that it is not in scope of data protection law may make it less useful for research.<sup>172</sup>

#### **Security measures for patient data**

All organisations using patient data are expected to have robust security systems and procedures in place.<sup>163,174</sup> Such measures may include encryption,<sup>175</sup> use of synthetic datasets,<sup>176</sup> or only allowing access to data at secure cloud computing facilities (POSTnote 629)<sup>177</sup>

### **Privacy and data sharing**

While use of patient data is governed by various rules and principles (Box 2), the use of large amounts of data to develop AI systems raises questions over privacy. For example, in 2017, the Information Commissioner's Office (ICO) found that the Royal Free Hospital had failed to comply with data protection law after sharing identifiable patient data with DeepMind for development of a diagnostic system for kidney injury.<sup>178,179</sup> Some evidence suggests a lack of awareness among the public of how patient data are shared,<sup>180</sup> and public scepticism towards sharing it, particularly with industry. In a 2018 survey of 2080 UK adults, 50.3% were willing to share anonymised data with research institutions, while 12.2% were willing to share it with industry for healthcare improvement purposes.<sup>181</sup>

There is wide variation in the terms of existing data sharing agreements between the NHS and industry.<sup>28</sup> Some stakeholders have raised concerns that NHS leaders lack the expertise to negotiate data sharing agreements that reflect the value of the patient data held by the NHS.<sup>182</sup> In 2020, the UK Government established the NHSX Centre for Improving Data

Collaboration.<sup>183</sup> It aims to ensure data sharing partnerships are made for the benefit of the whole NHS.<sup>184</sup>

### **Data quality**

Large, high-quality training datasets are needed for AI systems to produce accurate outputs.<sup>93–95</sup> Inaccurate or incomplete data can lead to poor performance.<sup>1</sup> Data must also usually be in a structured digital format, which can easily be processed by an ML algorithm.<sup>22</sup> However, the quality and organisation of data varies widely between different NHS services, depending on the degree to which data are being recorded in electronic format.<sup>28</sup> For example, paper records are still common in secondary care.<sup>185</sup> In 2017, 54% of NHS trusts reported staff could rely on digital records for all the information they needed.<sup>186</sup> In addition, many IT systems used in the NHS are unable to communicate with other systems, making it difficult to connect them with AI software and to gather data in a consistent way.<sup>28</sup> The NHS Long Term Plan (and other frameworks)<sup>14,160,187</sup> prioritise the use of interoperability and data collection standards to tackle this issue. Under the plan, all NHS providers are expected to reach a 'core level of digitisation' by 2024.<sup>15</sup>

### **Security**

Commentators have raised concerns that widespread use of AI and other technologies in healthcare increases the potential for cyber-attacks on such systems ([POSTnote 554](#)).<sup>188</sup> The need to share large datasets with external developers during AI development may increase the risks of a data breach.<sup>189</sup> In addition, hackers or other bad actors may seek to manipulate an AI system's outputs to disrupt or defraud the healthcare system,<sup>190–192</sup> or to extract patient data used in training.<sup>189,193</sup>

### **Accountability and legal liability**

Surveys have reported various levels of public awareness and trust of AI and automated decision-making in healthcare and other areas,<sup>129,194–199</sup> with some concerned that AI could lead to unclear or reduced responsibility for decisions.<sup>194,195</sup> In a 2016 survey of 12,003 adults across 12 countries by PwC, 39% of UK respondents said they would be willing to engage with an AI system to get a diagnosis or treatment/health advice and 50% said they would not be willing to do so.<sup>199</sup> Currently, most AI systems provide recommendations to clinicians, who balance these against their own knowledge and experience. A series of Academy of Medical Sciences workshops with 53 patients and members of the public, recommended that AI should support, rather than overrule, decision-making by clinicians.<sup>130</sup>

From a legal perspective, if a recommendation from an AI system led to a patient being harmed by a clinician, the clinician, developer and healthcare provider could face criminal charges or civil claims. The clinician could also face professional disciplinary proceedings.<sup>200–207</sup> There is a lack of precedent for how these cases would be resolved, and no professional regulators have introduced guidelines for AI use. Professional bodies, including the Academy of Medical Royal Colleges, have noted concerns about the uncertainty around accountability and liability.<sup>2,208</sup> These issues are further complicated by the use of 'black box' systems,<sup>209</sup> whose complexity makes it difficult to fully understand how a decision has been reached ([POSTnote 633](#)).<sup>210,211</sup> Some stakeholders have argued that new legal mechanisms may be required for AI in the future.<sup>212–214</sup>

### **Health inequalities**

Depending on how they are developed and used, AI systems have the potential to reduce or increase health inequalities. For example, AI systems could reduce variations in care by providing more consistent recommendations of treatments and diagnoses, based on up-to-date medical advice.<sup>133,215,216</sup> However, there is a risk of AI systems exhibiting 'algorithmic bias', providing recommendations that discriminate against certain demographic groups ([POSTnote 633](#) Box 2).<sup>217–220</sup> This can arise from decisions made during development of an AI system, or use of training data that under-represent a certain group or reproduce historic biases. For example, one commonly used skin cancer research database mainly contains fair-skinned patient images. Some experts have suggested that ML systems trained using these images may have difficulty diagnosing cancers in patients with darker skin types.<sup>221,222</sup> Data protection law requires users of personal data to mitigate risks of discrimination.<sup>189</sup> The Equality Act 2010 prohibits decisions that discriminate on the basis of certain characteristics.<sup>223,224</sup>

### **Regulatory issues**

AI systems that have a direct medical purpose will qualify as medical devices, *in vitro* diagnostic devices, or active implantable devices.<sup>225–227</sup> In the UK, these are regulated by the Medicines and Healthcare products Regulatory Agency (MHRA).<sup>206</sup> EU device regulations that existed prior to the end of the Brexit transition period remain in place as 'retained EU law' under the European Union (Withdrawal) Act 2018.<sup>228,229</sup> The Government has published guidance on the requirements for placing medical devices on the market in Great Britain from January 2021.<sup>229</sup> Requirements differ in Northern Ireland. Future UK regulations will be developed under provision of the [Medicines and Medical Devices Bill 2019-21](#). The Government has indicated new regulations will aim to increase safety and be more responsive to new technologies, including AI.<sup>229,230</sup>

The use of personal data in AI systems is governed by the ICO.<sup>231</sup> There are extra safety standards for software used in the NHS.<sup>232,233</sup> Development of AI systems within the NHS is classed as medical research, and usually requires approval from the Health Research Authority.<sup>234</sup> The Care Quality Commission has stated that suppliers of any future AI systems that make diagnoses or treat patients without human intervention would need to be registered.<sup>235</sup> With many bodies involved, some stakeholders view existing regulatory processes as difficult to navigate and a barrier to innovation.<sup>236,237</sup> The NHS AI Lab is funding projects to streamline regulatory processes,<sup>20</sup> including the creation of a multi-agency advice service, which will provide a single point-of-contact for AI developers seeking guidance.<sup>238</sup>

Some ML systems present challenges under existing regulation; they continue to learn and optimise as they are given new input data.<sup>22</sup> There are questions around how such systems could be monitored to ensure they remain safe and effective.<sup>239</sup> The US Food and Drug Administration has proposed regulations that would allow developers to pre-specify a safe process for future changes to AI systems.<sup>240</sup> The British Standards Institution is working with a US partner to consider how international standards for medical devices could be changed to meet the challenges posed by AI.<sup>241,242</sup>

## Rep. Buddy Carter signals support for federal privacy legislation

By [BEN LEONARD](#)

01/26/2021 01:58 PM EST

Rep. Buddy Carter signaled support on Tuesday for federal tech privacy legislation, indicating a willingness to work with the Biden administration on such a measure.

Carter (R-Ga.), who sits on the House Energy and Commerce tech subcommittee, said at a Tuesday POLITICO Live event on ethics and artificial intelligence that “we need to look at” privacy legislation, saying it could ease concerns and build public confidence in AI.

Currently, the United States does not have a federal digital privacy law on the books, leaving [tech data available in some cases, for example, to the U.S. military as well as foreign nations](#). [There is also no robust government oversight of AI algorithms](#), allowing tech firms to call the shots. Lawmakers have previously voiced [bipartisan concerns about facial recognition technology and other AI-related concerns](#), but [broad federal privacy legislation has stalled](#).

Carter cited concerns about artificial intelligence in light of China’s broad use of AI facial recognition and other technology for surveillance.

“People are naturally and rightfully concerned,” Carter said. “In order for it to succeed, we’ve got to have a buy-in if you will by the general public. We need them to have confidence in that.”

Carter emphasized that he wants the government to not have “that strong” of a role, but said he understood that the government will have to have some role in regulation.

“The benefits of AI are enormous. There are risks, there’s no question about it. And we’ve got to understand and know how we’re going to manage those risks,” Carter said.

Carter acknowledged finding support for increased regulation might be hard to find among the GOP caucus, though.

The European Union implemented its own privacy law in 2018, but [concerns about a lack of enforcement have remained](#). The U.S. has lagged behind the Europe in privacy, Terrell McSweeney, a Federal Trade Commission commissioner from 2014-2018 and current partner at Covington & Burling LLP, said at the event Tuesday.

Carter also said he is committed to working with the Biden administration on tech issues. Working with the EU can help to alleviate fears about AI, he said.

“We need to work with the European Union,” Carter said. “Russia and China are not our friends. There are a lot of good things that can come out of AI ... but there is also a lot of bad things. We’ve got to get past that fear ... and we’ve got to move forward.”

Panelists at the event called for a more unified approach to privacy regulation. An alliance on tech between the EU and the United States faces major impediments, with [the two entities not agreeing on some key policy issues](#).

“It doesn’t mean we have to come up with the same exact regulatory frameworks globally,” McSweeney said. “I’m hopeful that because the new administration is really committed to working with our allies we can reset the conversation with Europe a little bit. We’re at an early enough stage, especially with regards to AI, that we can start to bring some of these ideas together.”



## Believe it or not, the U.S. has something to teach Europe about privacy

By Vincent Manancourt, Mark Scott

02/10/2021 06:01 AM EST

BRUSSELS — Europe touts its data protection rules as the "[gold standard](#)." But when it comes to enforcement, it's got nothing on the U.S.

Since May 2018 — when the European Union's new data protection standards came into force — the U.S. has raked in almost \$6 billion in privacy fines, including hefty penalties for some of the biggest names in tech. The EU, meanwhile, has [collected just \\$329.8 million](#).

That's down to the Federal Trade Commission, the U.S. regulator in charge of enforcing the country's privacy rules as well as a portfolio of other powers that includes consumer protection and antitrust enforcement.

"The FTC is a superior enforcement regime," said Jessica Rich, a former director of consumer protection at the FTC. "It comes down to focus. GDPR [the [EU's General Data Protection Regulation](#)] is more about regulation, the U.S. approach is more enforcement-focused."

Washington's stance could be about to get a whole lot tougher.

Under the administration of President Joe Biden, the U.S. watchdog will swing to the Democrats — a party historically more eager to rein in big business than the Republicans, which controlled the FTC under former President Donald Trump. Potential candidates to fill one of the FTC commissioner roles include Lina Khan, an antitrust expert and [staunch critic of the big tech companies](#), though nominations have yet to be made.

Evidence of American toughness on privacy, at least regarding enforcement, may come as a shock to those used to hearing that Washington is miles behind Brussels. EU officials [have been eager](#) to trumpet the bloc's privacy regime as the world's strictest and a model for countries from Brazil to South Korea.

That image has been reinforced by [European courts repeatedly ruling](#) that the U.S. [isn't safe enough](#) to store European data. But for eagle-eyed observers of privacy on both continents, that's a false framing of the transatlantic divide.

"This narrative that Europe is leading way ahead of the U.S. is ridiculous. Europe has privacy on the books, but the U.S. has a lot of privacy on the ground," said Omer Tene, vice president of the International Association of Privacy Professionals.

The stats back up his assessment.

The FTC [handed Facebook a \\$5 billion levy](#) in 2019 for its role in the Cambridge Analytica scandal — its biggest ever fine. By comparison, the biggest privacy fine issued in the EU is €50 million, or roughly \$60 million — 100 times smaller — [by the French regulator](#) against Google for failing to gather sufficient user consent when displaying targeted ads.

## Regulating Big Tech bigly

In Europe's defense, many national regulators did not have enforcement powers until the new privacy rules came into effect in 2018. Now, a series of investigations into the likes of Apple, Facebook and Google are underway across the bloc. WhatsApp, the messaging app owned by Facebook, [is on deck for a privacy fine](#) of between €30 million and €50 million from Ireland's data protection agency in a decision expected by the late summer.

Still, the FTC's hit list since 2018 dwarfs Europe's.

Alongside the Facebook fine, [YouTube paid \\$170 million](#) in 2019 for violating children's privacy, and Equifax, the credit-checking company, [had to shell out \\$575 million](#) in the same year for a nationwide data breach. Even Chinese-owned app [TikTok coughed up \\$5.7 million](#) for illegally collecting children's online information.

The U.S. watchdog has also been quick to target companies that have become household names during the coronavirus pandemic, such as videoconferencing app Zoom, [which it ordered to improve data security in late 2020](#).

There are limits to the FTC's fining powers, including that it can sanction companies only for a second violation of U.S. law. Plenty of Silicon Valley critics also note that Facebook's fine hasn't stopped many of its data-hungry practices. But even when the Washington watchdog can't hit companies directly in the pocket, the FTC has forced wholesale changes to the way organizations deal with data, something that has so far largely eluded Europe's agencies.

"They require companies to proactively change their practices, create new internal policies, procedures, controls and have in place internal and external audits, checks and balances," said [Markus Heyder](#), a former FTC official and now vice president of the Centre for Information Policy Leadership, a Washington-based think tank. "These changes are much more effective, have larger impact on organizations and are ultimately more privacy-protective going forward than fines alone. They effectuate real change."

The FTC's enforcement has often been at the cutting edge of how tech is being used.

[In a case earlier this year](#), the U.S. agency forced a facial recognition company to delete not only training data like photos and videos, but also the "face embeddings," a technical term for features used for facial recognition, as well as the relevant algorithms and models used.

The case was praised across Europe, with Dutch privacy expert Mireille Hildebrandt saying it could be a watershed moment in tackling invasive tech — and a wake-up call to the 27-country bloc's own privacy enforcers.

“We should not be complacent about our legal framework,” Hildebrandt said, referring to Europe’s privacy rules. “The GDPR is far more effective, because it does not depend on [terms of service] but on the law itself. However, I do believe that civil society in the U.S. is more vigilant and the U.S. may actually move ahead of us precisely because they are in many ways far behind.”

## Legislation incoming

The lack of a comprehensive federal privacy law in the U.S. — at the root of many unfavorable comparisons with the EU — could also be about to change. The pandemic has pushed privacy up the agenda, prompting states like Virginia, New York and Washington to press ahead with state-based privacy frameworks, as California has already done.

But action at the state level, which is only expected to pick up momentum, could also prompt Congress to move faster on its own privacy framework, although issues around how national legislation would work alongside U.S. state rules still need to be hammered out. Speaking to POLITICO, Democratic Sen. [Ron Wyden](#) of Oregon highlighted privacy as a key priority for U.S. lawmakers.

"We're seeing these shady data brokers and governments practically every week finding new ways to get the personal information and put at risk the well-being of Americans without complying with the Constitution. You shouldn't be able to buy your way around the Constitution," he said.

Obstacles in Congress exist, however. Unless Democrats eliminate the filibuster — which requires a 60-vote majority to pass most legislation in the Senate — advancing most notable tech bills [will remain an uphill battle](#) even though they now control the upper chamber.

Still, early indications suggest that privacy could be a higher priority in Biden's administration than it was for Trump. Other issues, notably the Covid-19 pandemic and associated economic recession, may still make it tough to get data protection proposals onto the legislative agenda.

The new U.S. president moved quickly to designate a lead negotiator for a privacy deal with Europe. Vice President Kamala Harris has first-hand experience tackling consumer privacy issues from when she was California’s attorney general. Her successor in that role, Xavier Becerra, who’s been enforcing California's recently enacted GDPR-like law, is also joining the new administration as the nominee to be Biden's health secretary.

A shift in the balance of power at the FTC — Democrats will eventually have three commissioners to the Republican’s two — could also see it ramp up privacy enforcement. Yet,



as Washington has turned against the tech companies, both sides of the aisle have taken up the call for beefed-up privacy standards.

“Privacy is not a partisan issue, but the Democrats have more regulatory zeal,” said the IAPP’s Tene.

*Cristiano Lima contributed to this report.*