ELECTRONIC FRONTIER FOUNDATION

May 6, 2021

VIA ELECTRONIC FILING

Roger Severino, Director
U.S. Department of Health and Human Services
Office for Civil Rights
Attention: RFI, RIN 0945-AA00
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201

RE: Department of Health and Human Services, Office for Civil Rights
RIN 0945-AA00, Docket No. HHS-OCR-0945-AA00

To Whom It May Concern:

Thank you for the opportunity to provide written comments to the Department of Health and Human Services, Office for Civil Rights, on its Request for Information [HHS-OCR-0945-AA00] regarding modifying Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules to improve coordinated care. We write in support of the privacy protections in HIPAA, but with privacy concerns about several of the proposed modifications.

Over the past 30 years, the Electronic Frontier Foundation (EFF) has been the leading nonprofit defending digital privacy, free speech, and innovation. EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

Before delving into the questions presented in the RFI, we address two threshold issues. First, we are disturbed that the RFI repeatedly frames parts of HIPAA's privacy and security rules as "regulatory burdens." Viewing privacy and security as burdens on the health care system treats patients as data and forgets about them as people. What people believe and whom they trust matters (think masks and vaccines). Patient privacy and trust are intrinsic to medicine. Quality healthcare relies on patients to fully disclose symptoms to properly assess, diagnose, and treat the medical issues at hand. Since the passage of the Privacy Rule and Security Rule, HIPAA has protected highly sensitive and confidential personal health information for patients, resulting in patient confidence that personal health information is protected.

The RFI is considering shifting treatment decisions away from patients and lowering the bar for PHI disclosure. If implemented, patients will no longer know where their PHI has been distributed and may suffer long-term consequences if the information is obtained by an entity not covered by HIPAA. If patients believe that their health information is being shared without their knowledge or approval, many will not disclose their symptoms or

medical issues, resulting in delayed medical care, which will ultimately increase the cost of healthcare.[1]

Second, we fear that the RFI is blaming "regulatory burdens" supposedly associated with patient privacy or security for existing, unrelated imperfections in our health care system. Some of the difficulty providers and patients encounter is a result of misinformation and misunderstanding of HIPAA. HIPAA is already flexible enough to allow much of the RFI's specific concerns. Covered Entities (CEs) already may disclose information for reasons of Treatment, Payment, Operations (TPO), to family members, and in cases of emergency. Health care providers already may disclose PHI to another healthcare provider as needed for treatment;[2] a health care provider already may disclose PHI to a non-HIPAA-covered service provider as needed for the coordination and management of treatment.[3] Additionally, HIPAA already provides that family, friends, and others may obtain PHI without the patient's permission in several cases.[4]

The "barriers" and "burdens" that the RFI asserts are at least partly due to fear and misunderstanding. As a former Director of the Office of Civil Rights stated, "there is anxiety about our rules in all the wrong places."[5] OCR's focus in resolving complaints and violations is on broad-based security threats, not permitted disclosures.[6] In a 2015 Congressional hearing addressing misinformation regarding permissive disclosure under HIPAA,[7] one witness said, "Doctors have the fear of God placed before them because of

---

[1] As a longtime participant in California health policy discussions, EFF has heard health IT proponents repeatedly complain that Part 2 substance abuse requirements or state constitutional privacy protections for sensitive health information relating to mental illness or the exercise of reproductive health rights are inconvenient. But such protections are important to vulnerable populations, including patients with Severe Mental Illness (SMI), Substance Abuse Disorder (SUD), and other marginalized communities.

[2] 83 Fed. Reg. 64302.

[3] 45 C.F.R. §§ 164.501, 164.502(b)(2)(i).

[4] 45 C.F.R. 164.510; *e.g.*, when the patient has been given the opportunity to object but does not, when the patient poses a danger to self or others, in case of emergency, and when the patient lacks capacity to consent or object.

[5] "Does HIPAA Help or Hinder Patient Care and Public Safety": Hearings on HIPAA Before the Subcomm. on Energy & Commerce, 113th Cong. (2013) (available at https://www.c-span.org/video/?312392-1/dhhs-official-testifies-hippa-privacy-rules) (León Rodríguez, former director of the Office of Civil Rights at the Department of Health and Human Services).

[6] *Id.*

[7] The Helping Families in Mental Health Crisis Act: Hearings on H.R. 2646 Before the Subcomm. on Energy & Commerce, 114th Cong. (2015) (available at https://energycommerce.house.gov/committee-activity/hearings/hearing-on-examining-hr-2646-the-helping-families-in-mental-health).

hospital CEO's and also personal injury lawyers."[8] This statement exemplifies both the fear and misinformation pervasive in the health industry–there is no private cause of action under HIPAA, so personal injury lawyers could not pursue claims under HIPAA.

Eliminating privacy protections to address misinformation and misplaced fear will not help our health care system.

## DISCUSSION AND COMMENTS

### 1. The RFI's Core Concepts of Care Coordination and Case Management Are Not Defined

The proposed rule would expand the definition of "health care operations" to include disclosures and uses for "care coordination" or "case management"—but the NPRM then leaves those two terms at best vaguely defined. The NPRM provides 4 definitions for care coordination and 2 definitions for case management. Some of these definitions are so broad and ambiguous that almost any activity could be covered.[9] In other words, the interplay between these undefined and redefined terms could swallow the consent requirement for many use and disclosure decisions.

---

[8] *Id.* (Dr. Jeffrey Lieberman, Chairman of the Department of Psychiatry at Columbia University).

[9] Additional care coordination definitions in RFI: Department's Office of Inspector General: "coordination and management of care as the deliberate organization of patient care activities and sharing of information between two or more value-based enterprise (VBE) or VBE participants and patients, tailored to improving the health outcomes of the target population, in order to achieve safer and more effective care for the target population"; Center for Medicare & Medicaid Services: Services furnished to assist individuals, eligible under the (Medicaid) state plan who reside in a community setting or are transitioning to a community setting, in gaining access to needed medical, social, educational, and other services; Agency for Healthcare Research and Quality (AHRQ) defines care coordination as, "The deliberate organization of patient care activities between two or more participants (including the patient) involved in a patient's care to facilitate the appropriate delivery of health care services"; and, for case management, American Case Management Association defines it as, "A collaborative practice model including patients, nurses, social workers, physicians, other practitioners, caregivers and the community."
An additional case management definition in the RFI: American Case Management Association defines it as, "A collaborative practice model including patients, nurses, social workers, physicians, other practitioners, caregivers and the community." (NPRM pgs. 15-19).

To illustrate, the National Quality Forum (NCQ) defines care coordination as a:

> [M]ultidimensional concept that includes effective communication among healthcare providers, patients, families, and caregivers; safe care transitions; a longitudinal view of care that considers the past, while monitoring present delivery of care and anticipating future needs; and the facilitation of linkages between communities and the healthcare system to address medical, social, educational, and other support needs that align with patient goals.[10]

Phrases like "anticipating future needs" are quite broad. Patients suffering from SUD or SMI may disclose concerns about future emotional or other support to their providers as they apply to schools or for jobs and housing. Are providers free to disclose those concerns to others under the rubric of care coordination? Who decides "patient goals"?

As another example, the Case Management Society of America (CMSA) defines case management as a:

> Collaborative process of assessment, planning, facilitation, care coordination, evaluation, and advocacy for options and services to meet an individual's and family's comprehensive health needs through communication and available resources to promote patient safety, quality of care, and cost-effective outcomes.[11]

The patient's role here is again unclear in a supposedly "collaborative" process. Imagine a patient who suffers from serious anxiety, causing them to miss a few appointments. Under this expansive view of case management, might a provider unilaterally disclose the patient's anxiety to others in a well-meaning attempt to "promote quality of care"? Once such facts are disclosed to entities that are not CEs, the information can spread throughout the economy, potentially affecting credit scores and other metrics routinely used by businesses for hiring, housing or insurance.

The harm of the definition's vagueness is worsened by the RFI's proposal to exempt both care coordination and case management from the minimum necessary rule. This makes no sense and will magnify patients' concerns that their sensitive health data will be widely disclosed without meaningful privacy protections.

In turn, patients will be less likely to seek treatment since they fear disclosure of PHI. Currently, only 2.5 million of the 21.2 million people suffering from mental illness seek

[10] NPRM at 18.
[11] NPRM at 19.

treatment.[12] The human and economic toll is enormous: untreated mental illnesses in the U.S. cost more than $100 billion a year in lost productivity.[13] If the privacy rule is weakened, such patients may be even more deterred from seeking treatment out of fear that any diagnosis will lead to prejudice, discrimination, and stigma, with consequences for their families as well.

2. Lowering the Standard of Disclosure to "Good Faith Belief" Addresses the Wrong Issue

The RFI proposes to change the privacy standard that allows CEs to use or disclose some PHI based on their "professional judgment" to a standard of the CE's "good faith belief" that such use or disclosure is in the individual's best interest. EFF opposes this proposed replacement standard.

Patients and patient advocates are "almost universally opposed" to this change.[14] Existing law already authorizes CEs to disclose patient information in many of these situations. Unfortunately, misinformation about the risks of disclosing data under HIPAA may be one of the most important reasons that CEs sometimes fail to disclose. Congressional committees have over the years heard witnesses testify that they felt the doctors would disclose if it were not for the risk of violating HIPAA.[15]

Given that the standard already allows many of these disclosures, it is unclear whether lowering the standard would actually help. It is not hard to imagine common, recurring situations where patients and certain family members disagree about the best interests of the individual. Patients and their families may have greatly divergent views of proper care or treatment for mental health, substance abuse, sexual orientation, gender assignment, or reproductive health issues.

---

[12] Sara Heath, *Understanding Stigma as a Mental Healthcare Barrier*, PATIENT ENGAGEMENT HIT (June 8, 2017), https://patientengagementhit.com/news/understanding-stigma-as-a-mental-healthcare-barrier?utm_content=b1281c3eaa9e820f79ecee0fe1311937&utm_campaign=MHD%25206%252F8%252F17&utm_source=Robly.com&utm_medi.

[13] The Editors, *The Neglect of Mental Illness Exacts a Huge Toll, Human and Economic*, SCIENTIFIC AMERICAN (Mar. 1, 2012), https://www.scientificamerican.com/article/a-neglect-of-mental-illness/.

[14] NPRM pg. 142 ("Commenters who identified as patients or privacy advocacy groups almost universally opposed modifying the Privacy Rule to expand permitted disclosures of information related to SMI and opioid use disorder or other SUDs").

[15] The Helping Families in Mental Health Crisis Act: Hearings on H.R. 2646 Before the Subcomm. on Energy & Commerce, 114th Cong. (2015) (available at https://energycommerce.house.gov/committee-activity/hearings/hearing-on-examining-hr-2646-the-helping-families-in-mental-health).

These issues have historically been acute for substance abuse. The existence of 42 C.F.R. Part 2 is recognition that in this society, a pervasive stigma around issues of SUD and SMI can lead to patients' facing discrimination in obtaining housing or employment. It is no accident that more than a few programs for substance or alcohol abuse have "anonymous" in their name; confidentiality can be a cornerstone to recovery, because it helps patients themselves engage in honest disclosure, which in turn can facilitate a sense of community based on trust.[16]

Finally, we do not see how the proposed rule can be properly policed by patients. The rule does not require that a CE adequately document its decision to disclose under the "good faith" standard. The patient would appear to bear the burdens of challenging the CE and of proving bad faith—yet only the CE would have the critical information.

During these times of misinformation regarding public health issues, e.g., COVID, anti-vax movements, and suspicious home remedies found on social media, the health industry needs to maintain and build upon the trust they currently have. Privacy protections are at the heart of such trust. It is ultimately the patient who must suffer the consequences of well-intentioned but misinformed decisions regarding their care.

3. The Proposed "Reasonably Foreseeable" Standard for Emergency Disclosures is Too Permissive

The RFI proposes to change the standard for disclosures of PHI in an emergency from "serious and imminent" to "serious and reasonably foreseeable." But "reasonably foreseeable" is too weak a standard for emergency disclosures. The notion of "imminence" limits the expected harm to the immediate or very near future, but it also invokes a notion of certainty, that the harm is surely impending. If a person is a regular cigarette smoker, serious health harms can be reasonably foreseen, but is each instance of cigarette smoking an emergency? When one thinks of the potential for health interventions in the area of food, drink, and other lifestyle choices, the "reasonably foreseeable" standard seems to confuse wellness programs with emergencies.

The "reasonably foreseeable" standard is also more discretionary than "imminent." The notion of "reasonableness," anchored in the common law of negligence in tort, has long relied on the reporting of judicial decisions in concrete cases for its nuanced meaning. Absent scrutiny of how CEs in practice interpret "reasonably foreseeable," we anticipate wildly varied reasons for "emergency" disclosures, and significantly more unnecessary data disclosure.

[16] Attending a treatment center requires a willingness to receive treatment services. Disclosing PHI to the family does not mean the patient would necessarily agree with the family's desires or judgment. Such disclosure might not only harm the patient's trust in treatment, but also produce tension between patient and family.

4. Expanding the Right of Access to Extend to Personal Health Applications Will Likely Increase the Flow of Health Data to Non-HIPAA Entities.

Although we generally support patient access to PHI, we do not support unfettered patient access for sharing of PHI for personal health applications. The proposed amendments will likely result in more intimate, sensitive, and highly valuable information being sent to entities not covered by HIPAA. The rise of electronic health records and medical/health "wearables" has created a huge legal Wild West for individual data pertaining to one's health or genetics stored with or collected by non-HIPAA businesses, especially because most ordinary persons have no idea that HIPAA's legal protections turn on "covered entity" status.

Over the past decade, downloads of mobile health (mHealth) apps have been on the rise.[17] Technology firms increasingly want a bigger share of the more than $3 trillion spent annually on health care in the United States.[18] 65% of smartphone users have an mHealth app on their phone.[19] mHealth apps purport to support consumers in their pursuit of health goals, such as weight management,[20] stress management,[21] smoking

[17] Aaron Smith, *Record shares of Americans now own smartphones, have home broadband*, PEW RESEARCH CENTER (Feb. 19, 2020), https://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/; *See also* Statistical Report, Number of connected wearable devices worldwide by region from 2015 to 2022, STATISTA (Feb. 19, 2020), https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/.

[18] Natasha Singer, *How Big Tech Is Going After Your Health Care*, THE N.Y. TIMES (Dec. 26, 2017), https://www.nytimes.com/2017/12/26/technology/big-tech-health-care.html.

[19] Mindsea Team, *25 Mobile App Usage Statistics To Know In 2019*, MINDSEA, https://mindsea.com/app-stats/.

[20] Brianna Elliott, *The 10 Best Weight Loss Apps That Help You Shed Pounds*, HEALTHLINE (Sept. 11, 2017), https://www.healthline.com/nutrition/10-best-weight-loss-apps.

[21] Lizzy Francis, *10 Stress Management Apps to Help During Hard Times*, YAHOO! (Mar. 24, 2020), https://www.yahoo.com/lifestyle/10-stress-management-apps-help-191014172.html.

cessation,[22] self-management of health conditions,[23] and, more recently, social-distancing measures in light of COVID-19.[24]

The private information that a user enters into medical apps is collected, shared, or sold, often without the user's knowledge or consent.[25] A 2014 Federal Trade Commission (FTC) study revealed that 12 mHealth apps and devices transmitted information to 76 different third parties, and some of the data could be linked back to specific users; in addition, 18 third parties received device-specific identifiers, and 22 received other key health information.[26] Information about some of the most private and sensitive aspects of people's lives is available for analysts, data brokers,[27] and government entities (both domestic and foreign) to examine without a patient's knowledge or consent.

Technology companies have also entered the medical information market. Xealth developed an application that is embedded in patients EHR that provides a list of possible health products; the doctor can go through that list and recommend particular products to

---

[22] Jessica Timmons, *The Best Quit Smoking Apps of 2019*, HEALTHLINE (Apr. 25, 2019), https://www.healthline.com/health/quit-smoking/top-iphone-android-apps.

[23] Technical Brief, *Mobile Applications for Self-Management of Diabetes*, US DEP'T OF HUM. & HEALTH SERV. (May 8, 2018), https://effectivehealthcare.ahrq.gov/products/diabetes-mobile-devices/technical-brief.

[24] Eliza Strickland, *An Official WHO Coronavirus App Will Be a "Waze for COVID-19"*, IEEE SPECTRUM (Mar. 20, 2020), https://spectrum.ieee.org/the-human-os/biomedical/devices/who-official-coronavirus-app-waze-covid19.

[25] Jay Hancock, *Workplace wellness programs put employee privacy at risk*, CNN (Oct. 2, 2015), https://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/index.html.

[26] Sarah Kellogg, *Every Breath you Take: Data Privacy and Your Wearable Fitness Device*, WASH. LAW., https://www.dcbar.org/barresources/publications/washington-lawyer/articles/december-2015-data-privacy.cfm.

[27] *See generally* Data Brokers: A Call for Transparency and Accountability, FTC Rep. 8, 46 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-reportfederal-trade-commission-may-2014/140527databrokerreport.pdf. Data brokers consolidate personal information for various commercial purposes, such as utilizing predictive analytics to discriminate among consumers regarding their race, economic status, and propensity to default or engage in crime. At that time, one database had information on 1.4 billion consumer transactions and more than 700 billion aggregated data elements; another data broker's database covered one trillion dollars in consumer transactions; and yet another data broker was adding three billion new records each month to its database. *Id.* at 47.

their patient; then, this list is sent to a vendor.[28] Amazon's program, Comprehend Medical, which is sold to hospitals, pharmaceutical companies, researchers, and other health care providers, uses data-mining techniques to look for trends in patient EHRs that doctors may not notice.[29] Meanwhile, Apple has created the Medical Health App to make it easier for users to access their own medical records. As privacy protections on PHI weaken, more companies can be expected to seek more of this sensitive and confidential information.[30] Correspondingly, patients will increasingly lose control of their PHI, and suffer the predictable consequences.[31]

Today, 80% of medical health records are in electronic format.[32] Most ordinary Americans don't know, however, that while HIPAA protects their privacy when their health data is held by or behalf of their direct treatment provider, it simply doesn't apply when they share their data with a company like Amazon or Apple, no matter how many health apps are on their iPhone or Apple Watch.

That basic legal distinction is only the tip of the iceberg. App and device policies, practices, and permissions can be confusing and unclear. Depending on where the PHI is stored, other applications may grant themselves access through their permissions. Each app typically has a list of permissions that are granted to the developer when the user downloads an app to a device, which users often do not understand. Unfortunately, permissions have serious consequences because many apps can access data on one's device that is unrelated to what the app is supposed to do.[33] In a study of 99 apps, researchers found that free apps included more unnecessary permissions than paid apps.[34]

---

[28] Anna Wilde Mathews, *Sharing Your Digital Health: New Rules Ease Access*, THE WALL STREET JOURNAL (Mar. 9, 2020), https://www.wsj.com/articles/sharingyourhealthdatanewdigitalrules-11583702453.
[29] *Id.*
[30] *Id.*
[31] Mark Andrus, *The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual*, THE AM. BAR ASS'N (Sept. 28, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/06_andrus/.
[32] Anna Wilde Mathews, *Sharing your Digital Health Data: New Rules Ease Access*, THE WALL STREET JOURNAL (Mar. 9, 2020), https://www.wsj.com/articles/sharingyourhealthdatanewdigitalrules-11583702453.
[33] The classic example is the "flashlight" app. *See, e.g.*, *Why Do Android Flashlight Apps Need Dozens of Permissions?*, EXTREMETECH (Sept. 12, 2019), https://www.extremetech.com/mobile/298363-why-do-android-flashlight-apps-need-dozens-of-permissions (flashlight apps have been found to "access your fine-grained location data, control Bluetooth connections, record audio, download data without notification, and write to your contacts list.").
[34] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 428 (2018).

If PHI is stored on such a device that also has an app with overbroad permissions, the PHI can be obtained.

Finally, federal regulatory authority in this area is splintered and confusing. The non-HIPAA technology firms are largely regulated by the Federal Trade Commission (FTC), which generally intervenes when the company does not adhere to its own privacy policy or essentially offers no security.[35] The Food and Drug Administration (FDA) generally has broad authority to regulate products marketed to the public, including medical devices under the Food, Drug, and Cosmetic Act (FDCA).[36] Although phones and wearables have been used to monitor health, the FDA has limited their jurisdiction to devices implanted in a patient's body (i.e., implantables).[37]

## CONCLUSION

A major lesson of this pandemic is that people's trust in the health care system is critical to health care outcomes. We have seen this in the context of advice about testing, about wearing masks, about social distancing, and about vaccination. While the RFI's most glaring problem is that two crucial concepts in this proceeding—"care coordination" and "case management"—have no clear meaning, our greatest disappointment is that the Department seems to be promoting more, and less accountable, disclosure of PHI without patient knowledge or consent. This will not promote patient trust, and the RFI will not improve health outcomes.

Respectfully submitted,

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation

Alex Moss
Staff Attorney
Electronic Frontier Foundation

Kenny Gutiérrez
Bridge Fellow
Electronic Frontier Foundation

---

[35] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 250 (3d Cir. 2015); Complaint at 2, *In re Trendnet Inc.*, FTC File No. 122 3090 (Jan. 16, 2014) (No. C-44), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[36] 21 U.S.C.A. § 321(h) (medical device means "any product intended for use in the diagnosis of disease or of the body.").

[37] 21 C.F.R. 880.6300; *see also* Caroline Saunders, *Balancing Innovation and Regulation: Why the FDA should adopt a More Dynamic Risk-Based System for Wearables*, 58 JURIMETRICS: J.L., SCI. & TECH. 83 (2017).