CENTER FOR DEMOCRACY & TECHNOLOGY

June 3, 2019

Alexandra Mugge et al.
Centers for Medicare & Medicaid Services
Department of Health & Human Services

Re: **CMS–9115–P**

Comments of the Center for Democracy & Technology on Interoperability, Patient Access, and Privacy

Dear Ms. Mugge,

The Center for Democracy & Technology (CDT) is pleased to comment on the Centers for Medicare and Medicaid Services (CMS)'s proposed rule on interoperability and patient access to electronic health information (EHI).[1] CDT is a nonprofit technology advocacy organization dedicated to promoting public policies that preserve privacy, promote innovation, and enhance individual liberties and equity in the digital age.

While CDT applauds the goal of giving patients better access to and ability to port their health information, we are concerned about the lack of privacy protections covering this sensitive information once it leaves the hands of an entity covered by the Health Insurance Portability and Accountability Act (HIPAA)[2] Privacy Rule.[3]

Health information, once outside of the possession of a HIPAA covered entity, is largely unregulated with respect to privacy protections, leaving people vulnerable to having their sensitive personal information repurposed, misused, and exploited or disclosed to their detriment.[4] The proposed rules seek to give effect to patients' choice and control over their information, but the commercial market for health data does not provide people with real choice or control. The consumer app ecosystem obfuscates people's ability to understand how various apps will use and share their data and to compare among apps' privacy practices.[5] By requiring covered entities

[1] Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally Facilitated Exchanges and Health Care Providers, 84 Fed. Reg. 7610 (proposed March 4, 2019) [hereinafter CMS proposed rule].
[2] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191, 110 Stat. 1936 (1996).
[3] 45 C.F.R. § 164.
[4] *See, e.g.,* Nat'l Comm. on Vital and Health Statistics (NCVHS), Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges 2-3 (Dec. 13, 2017), https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf.
[5] *See, e.g.*, Statement of Michelle Richardson, Director, Privacy & Data, Center for Democracy & Technology, before the U.S. Comm. on the Judiciary 14 (March 12, 2019), https://cdt.org/files/2019/03/FINAL-written-testimony-3.12-SJC-hearing.pdf; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013); Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A Journal of Law and Policy 543, (2008); Joel Reidenberg,

to provide access to EHI with no clear use or sharing limitations, the proposed rules shift the burden of protecting health information to patients and leaves them few legal tools to do so.

Rather than burdening patients with the impossible task of parsing apps' data practices, the Department of Health and Human Services (HHS) should use this interoperability initiative as an opportunity to incentivize better protections for health information outside of HIPAA. HHS can employ tools such as developer privacy agreements, assertions, and reporting mechanisms to hold non-covered entities accountable for their data practices. While these tools can help increase accountability, patients will not be able to safely and confidently transfer their health records outside of HIPAA-covered entities until Congress enacts comprehensive consumer privacy protections.

I. HHS should not double down on the notice and consent model that has failed to protect Americans' privacy.

HHS's goal of giving users more control over their health information and care is laudable. However, the proposed rules over-rely on the concept of user consent to dictate who can access EHI through an application program interface (API) and for what purposes.[6] HIPAA is designed to protect patients in part by limiting the disclosure of information to appropriate purposes and to the minimum necessary to accomplish the intended purpose.[7] While not perfect, this standard allows patients to transfer their records between providers without having to investigate each individual provider's policies and data practices. Once information leaves the hands of a HIPAA-covered entity, there is no such purpose limitation. While patients may be agreeing to share EHI with non-HIPAA entities to receive a particular health-related service, the EHI can be repurposed and shared in ways that far exceed the patient's control or expectations. Even when companies apply special protections to "sensitive health information," the definition is often much narrower than the scope of information that can be obtained through EHI and that is covered under HIPAA.[8] The proposed rules may give patients the illusion of control, but in reality they shift the burden of protecting EHI onto patients, who are not in a position to manage it.

The "notice-and-consent" model has failed to protect Americans' privacy in other sectors.[9] When people are deciding what apps and services to use, they do not face an array of high quality choices offering different but equally transparent privacy protections. Instead, people are expected to navigate an ecosystem of dense privacy policies, incomplete notices, and confusing settings, some of which are intentionally designed to get people to

---

Presentation, Putting Disclosures to the Test (2016), available at https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

[6] CMS proposed rule at 7621–22.

[7] CMS proposed rule at 7617; 5 C.F.R. § 164.502(a)–(b).

[8] *See, e.g.*, Network Advertising Initiative, Update to the 2015 NAI Code of Conduct 15 (June 2017), https://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf [hereinafter NAI Code of Conduct].

[9] *See, e.g.*, Woodrow Hartzog, *User Agreements are Betraying You*, Medium (June 5, 2018).

agree to share personal information without understanding what they're agreeing to.[10] Even if notices could offer complete clarity, no one has the time or cognitive capacity to read and compare them all.[11] In many cases, people need to use a particular company's app or product. This is especially likely in the health sector, where patients may be relying on a niche or patented service or receiving specific app recommendations from their doctors. Further, patients' EHIs can contain information about other people, such as family members, who have no opportunity to consent to the sharing.

While APIs are a common and convenient way of sharing information, API access is frequently exploited because neither the API owner nor the data subject has a full view or control of how data is used once it's shared. The information used in Cambridge Analytica's voter manipulation campaign was originally obtained through Facebook's API with user consent.[12] Social media APIs have also been used to surveil the Black Lives Matter movement and other First Amendment activity.[13]

Nearly every week brings a new revelation about an app sharing sensitive personal information with third parties unbeknownst to its users. One New York Times investigation revealed that many apps offering location-based services (where users agree to share their location in exchange for a service like navigation or location-based weather) share location data with third parties.[14] Location data can end up in the hands of bounty hunters,[15] law enforcement,[16] and abusive partners,[17] putting people in physical danger. A recent study reported that a range of health and wellness apps, including smoking cessation, fitness tracking, mental health, and ovulation tracking apps, had shared their users' sensitive information with third parties.[18]

---

[10] *See, e.g.*, Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You*, The Verge (Apr. 29, 2018), https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you; Brian Fung, *Lawmakers Want to Ban 'Dark Patterns,' the Web Designs Companies Use To Manipulate You*, Wash. Post (April 9, 2019), https://www.washingtonpost.com/technology/2019/04/09/policymakers-are-sounding-alarm-dark-patterns-manipulative-web-design-trick-youve-never-heard/?utm_term=.43b7b46a053c.

[11] *See* McDonald & Cranor, *supra* note 5.

[12] *See* Kurt Wagner, *Here's How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users*, Vox (Mar. 17, 2018), https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

[13] Matt Cagle, ACLU Northern California, *Facebook, Instagram, & Twitter Provided Data Access for Surveillance Product Marketed to Target Activists of Color* (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[14] Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, And They're Not Keeping It A Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[15] Joseph Cox, I gave a bounty hunter $300. Then he located our phone, Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[16] Seeltr from Sen. Ron Wyden to Randall L. Stephenson, President and CEO, AT&T (May 8, 2018), https://www.documentcloud.org/documents/4457319-Wyden-Securus-Location-Tracking-Letter-to-AT-amp-T.html.

[17] SeeTechnology Safety, Data Privacy Day 2019: Location Data & Survivor Safety (Jan. 28, 2019), https://www.techsafety.org/blog/2019/1/30/data-privacy-day-2019-location-data-amp-survivor-safety.

[18] *See* Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing & Privacy Practices of Smartphone Apps for Depression & Smoking Cessation*, J. Am. Med. Ass'n (JAMA) Netw Open. 2019;2(4):e192542 (Apr. 19, 2019), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=041919; Kari Paul, *Fitness & Health Apps May Be Sharing The Most Private Details About Your Life*, MarketWatch (March 5, 2019),

These privacy violations occur despite the fact that most apps initially request some sort of "consent" to access personal data. These "choices" do nothing to protect people from unexpected and harmful uses of their data. For most of this information, the only legal backstop is the Federal Trade Commission (FTC)'s authority to police unfair and deceptive trade practices, which the CMS proposed rule points to as a protection for patients' EHI.[19] However, the FTC has generally only pursued "deceptive" privacy actions in which it can prove that the company violated its own privacy policies, notices, or settings.[20] The agency does not impose affirmative and binding limits on companies' use or disclosure of data.[21] Moreover, the FTC lacks appropriate resources to engage in effective privacy enforcement, especially at the scale that would be necessary to adequately protect patients in API programs.[22]

II. Patients face serious risks of economic, physical, and emotional harm from the misuse of their health records.

The proposed rules do not adequately address the risk of harm to patients from the misuse of their EHI by unregulated entities. Both the CMS proposed rules and the Office of the National Coordinator for Health Information Technology (ONC) proposed rules acknowledge the risk of data breach and propose some measures to ensure data security.[23] But patients also face significant risks from the improper, opaque, or discriminatory use of their EHI to make decisions impacting their employment, credit, and other critical opportunities. Outside of HIPAA, EHI may be sold from health-related apps to third parties such as data brokers and insurers. Insurers are already using data from third parties, such as purchase and browsing history, and social media activity, to make decisions regarding eligibility, rates, and targeted marketing.[24] EHI could provide a wealth of detailed

---

https://www.marketwatch.com/story/fitness-and-health-apps-may-be-sharing-the-most-private-details-about-your-life-2019-02-26.

[19] CMS proposed rule at 7622.

[20] *See, e.g.*, Dave Perea, *FTC Privacy Enforcement Focuses on Deception, Not Unfairness*, MLex (Feb. 22, 2019), https://mlexmarketinsight.com/insights-center/editors-picks/Data-Protection-Privacy-and-Security/north-america/ftc-privacy-enforcement-focuses-on-deception,-not-unfairness; Müge Fazlioglu, *What FTC Enforcement Actions Teach Us About the Makings of Reasonable Privacy & Data Security Practices: A Follow-up Study*, Int'l Ass'n of Privacy Professionals (IAPP) (June 11, 2018), https://iapp.org/news/a/what-ftc-enforcement-actions-teach-us-about-the-makings-of-reasonable-privacy-and-data-security-practices-a-follow-up-study/.

[21] *See* Joseph Jerome, *Can FTC Consent Orders Effectively Police Privacy*, IAPP (Nov. 27, 2018), https://iapp.org/news/a/can-ftc-consent-orders-police-privacy/.

[22] *Id. See also, e.g.*, Harper Neidig, *FTC Says it Only Has 40 Employees Overseeing Privacy & Data Security*, The Hill (Apr. 3, 2019), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security.

[23] CMS proposed rule at 7635–36; 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 7424, 7427–28 (proposed March 4, 2019), https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02224.pdf [hereinafter ONC proposed rule].

[24] *See, e.g.*, Marshall Allen, *Health Insurers are Vacuuming Up Details About You—And It Could Raise Your Rates*, ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates; Jessica Baron, *Life Insurers Can Use Social Media Posts to Determine Premiums, As Long As They Don't Discriminate*, Forbes

health information to insurers that they otherwise wouldn't have access to, and patients could find their car, life, or home insurance rates going up based on their EKGs, ER visits, or genetic tests.[25]

The data broker and advertising industries have used inferred health information to target advertising in ways that could be harmful and exploitative. In 2013, research from the World Privacy Forum, presented in testimony before the Senate Committee on Commerce, Science, and Transportation, revealed that data brokers sold lists of people suffering from genetic diseases, dementia, HIV/AIDS, addiction, and cancer.[26] Sensitive categories have been used to target ads for payday loans, prescription drugs, crash diets, and other risky products.[27] Currently there is no law generally preventing companies from using health information for targeted marketing, and many companies include broad provisions in their privacy policies allowing them to use personal information to deliver personalized experiences. The Network Advertising Initiative's Code of Conduct instructs members (membership is voluntary) to obtain opt-in consent before using or inferring "sensitive health information."[28] However, the code delineates between sensitive and non-sensitive health conditions.[29] For example, it instructs that cancer is a sensitive health condition but "dental" and "vision" conditions and "cholesterol management" are not.[30] Thus, electronic health records contain a wealth of information that most patients would likely consider to be sensitive but that many advertisers view as fair game for targeted marketing.

Secondary use of EHI is likely to disproportionately harm patients who are most vulnerable to exploitation and discrimination. The menstrual and pregnancy tracking app Ovia has sold a paid version to employers that allowed them to track aggregate information about the pregnancies, health risks, and medical searches of their female employees using the app.[31] Credit card companies could use health and financial information from health records to target patients for high-interest healthcare credit card offers. Survivors of intimate partner violence

---

(Feb. 4, 2019), https://www.forbes.com/sites/jessicabaron/2019/02/04/life-insurers-can-use-social-media-posts-to-determine-premiums/#3364038d23ce.

[25] Angela Chen, *What Happens When Life Insurance Companies Track Fitness Data*, The Verge (Sept. 26, 2018), https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health; Michelle Andrews, *Genetic Tests Can Hurt Your Chances of Getting Some Types of Insurance*, NPR (Aug. 7, 2018), https://www.npr.org/sections/health-shots/2018/08/07/636026264/genetic-tests-can-hurt-your-chances-of-getting-some-types-of-insurance.

[26] Testimony of Pam Dixon, Executive Director, World Privacy Forum, before the Senate Committee on Commerce, Science, and Transportation (Dec. 28, 2013), http://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf.

[27] *See, e.g.*, Upturn, Led Astray: Online Lead Generation and Payday Loans (Oct. 2015), https://www.upturn.org/static/reports/2015/led-astray/files/Upturn_-_Led_Astray_v.1.01.pdf; Michael Corkery, *Google Sets Limits on Addiction Treatment Ads, Citing Safety*, N.Y. Times (Sept. 14, 2017), https://www.nytimes.com/2017/09/14/business/google-addiction-treatment-ads.html.

[28] NAI Code of Conduct at 15.

[29] *Id.*

[30] *Id.*

[31] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?*, Wash. Post (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.16ee258fe869.

are at a particularly high risk of being tracked with commercially available devices and data sources.[32] Information about healthcare visits (which can reveal not only treatment but also location information) and payment information can facilitate stalking and abuse.[33]

III. HHS can partially mitigate these risks by providing developer agreement language for APIs that limits the secondary use of EHI and by allowing API owners to seek assurances that developers are abiding by the agreements.

As discussed in Section I, API access is inherently vulnerable to misuse. In the absence of comprehensive consumer privacy protections, Americans rely on the architecture and policies of API programs to put reasonable boundaries around the use and sharing of data. After discovering that developers like Cambridge Analytica misused user data, Facebook overhauled its API policies to, for example, prevent developers from accessing data about users' friends.[34] There are two protective mechanisms in particular that HHS should consider: developer agreements and assurances.

Companies commonly provide APIs that allow third-party developers (or advertisers) to collect user information for certain permitted purposes; however, it is often infeasible to monitor what third parties do with the data once they have it. API providers address this limitation by requiring third parties to acknowledge terms or enter into agreements that condition API access.[35] For example, social media companies often prohibit API access for surveillance or law enforcement purposes.[36] Apple's HealthKit terms prohibit developers from using information collected through HealthKit for advertising; disclosing it to third parties without the user's express permission; and selling it to "advertising platforms, data brokers, or information resellers."[37] HHS can incentivize privacy without incentivizing blocking by providing standard developer agreement language for APIs. Regardless of their regular privacy policies, parties accessing APIs could agree to, for example, only use EHI to deliver the specific service requested by the patient and refrain from selling the data. Asking all third parties to agree to the same standards would preserve patient access and HHS's goal of preventing providers from blocking third parties on a case-by-case basis.

---

[32] *See, e.g.*, Rahul Chatterjee et al., *The Spyware Used in Intimate Partner Violence*, https://www.ipvtechresearch.org/pubs/spyware.pdf.
[33] *Id. See also* Nicki Dell et al., *How Domestic Abusers Use Smartphones to Spy on Their Partners*, Vox (May 21, 2018), https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google.
[34] *See, e.g.*, Sarah Perez, *Facebook Rolls Out More API Restrictions and Shutdowns*, TechCrunch (April 2018), https://techcrunch.com/2018/07/02/facebook-rolls-out-more-api-restrictions-and-shutdowns/.
[35] *See, e.g.*, Slack API Terms of Service, https://slack.com/terms-of-service/api, and Data Processing Addendum, https://slack.com/terms-of-service/data-processing; Apple HealthKit, Protecting User Privacy, https://developer.apple.com/documentation/healthkit/protecting_user_privacy [hereinafter Apple HealthKit privacy terms].
[36] *See* Twitter Developer Agreement and Policy, Part VII(A), https://developer.twitter.com/en/developer-terms/agreement-and-policy.html.
[37] Apple HealthKit privacy terms.

Developer terms need not impose any additional monitoring or enforcement responsibilities on providers, but they can provide an enforcement hook for the FTC. When a third party agrees to a set of terms as a condition of API access, the terms act as a representation in the same way that a privacy policy or notice would.[38] If the FTC finds that a non-HIPAA entity violated an API's terms, it can bring an enforcement action for deceptive trade practices. This would add additional weight to the CMS rule's statement that the FTC can protect patients' privacy where HIPAA does not apply.[39]

HHS should also consider allowing providers to voluntarily seek assurances or certifications that third parties are abiding by the API's terms. Assurances or certifications are a weak but standard method of encouraging compliance with developer terms. When API owners have reason to suspect that a third party is accessing or processing user data in ways that violate the API's terms, they can ask the third party for written assurances that (a) data was not used improperly and/or (b) any improperly obtained data was deleted. While assurances do not provide proof, they are representations that can also be used as an FTC enforcement hook. Further, if a provider seeks assurances and the third party does not respond within a reasonable time period, it should not be considered improper blocking for the provider to temporarily suspend the third party's API access until assurances can be obtained. Seeking assurances can be an entirely voluntary practice and need not impose additional liability on providers.

Conclusion

HHS should consider providing standard privacy terms for non-HIPAA entities accessing EHI APIs that limit the repurposing and disclosure of health records and allow providers to voluntarily suspend third parties for violating the terms. In the absence of meaningful consumer privacy laws, API terms of use and the ability to suspend violators are often the only lines of defense to protect privacy. While privacy terms of use and assertions are weak substitutes for legal privacy protections, they are bare minimum requirements for protecting patients' sensitive health information.

Sincerely,

Natasha Duarte
Center for Democracy & Technology
1401 K Street NW Suite 200
Washington, D.C. 20005
(202) 407-8822
nduarte@cdt.org

[38] *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 583, 628–34 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913&download=yes; Natasha Duarte, *The FTC-Venmo Privacy Settlement is All About Design*, Ctr for Democracy & Tech. (Mar. 1, 2018), https://cdt.org/blog/the-ftc-venmo-privacy-settlement-is-all-about-design/.
[39] CMS proposed rule at 7622.