epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Health and Human Services Department

Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement

86 Fed. Reg. 6446 / 86 Fed. Reg. 13683

May 6, 2021

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Health and Human Services Department (HHS) Notice of Proposed Rulemaking (NPRM) titled "Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement" published January 21, 2021.[1] HHS proposes to substantially modify the Standards for the Privacy of Individually Identifiable Health Information promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The main impact of HHS's proposed changes would be to reduce privacy protections for many patients, including particularly vulnerable individuals with stigmatized conditions.

Responding to specific requests for input, EPIC opposes changes to the HIPAA Privacy Rule that would weaken privacy protections for patients, authorize more widespread disclosure of Protected Health Information, and impose rigid opt in/opt out systems of case management that do

[1] 86 Fed. Reg. 6446, deadline extended to May 6, 2021 by 86 Fed. Reg. 13683.

not give patients meaningful control over their health data. EPIC recommends that the Department improve the standards for verification of patient identity.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values. Strengthening privacy protections under HIPAA is especially important in the Pandemic Era as the collection and surveillance of health and health-related data has expanded dramatically.[2] It is also important for HHS to ensure that evolving healthcare and case management technologies increase, rather than restrict, patients' ability to protect and control their personal information.[3]

I. EPIC's supports the Department's efforts to reduce Identity Verification Burdens, but urges a more comprehensive approach to reduce barriers to access.

HHS proposes to "modify paragraph (2)(v) of 45 CFR 164.514(h) to expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual (or his or her personal representative) exercising a right under the Privacy Rule."[4] The new rule would specify that requiring notarized requests to assert Privacy Rule rights is unreasonable, and would otherwise impose a "less burdensome verification measure" test for covered entities.[5] EPIC supports the Department's efforts to reduce the burden on patients, particularly encouraging widespread access to

---

[2] *See* Alan Butler & Enid Zhou, *Disease and Data in Society: How the Pandemic Expanded Data Collection and Surveillance Systems*, 70 Am. U. L. Rev. ___ (forthcoming 2021), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836914.

[3] *See*: FOIA Request to Department of Health and Human Services Re: Privately Obtained Covid-19 Patient Information (Apr. 8, 2020), https://epic.org/foia/hhs/covid-19/EPIC-20-04-08-HHS-FOIA-20200408-Request-Health-Tech-Memo.pdf; Comments of EPIC to Department of Health and Human Services HIPAA Privacy Rule and the National Instant Criminal Background Check System (NICS), 78 Fed. Reg. 23 (codified at 45 CFR Parts 160 and 164) (Jun. 7, 2013), https://epic.org/apa/comments/EPIC-HHS-HIPAA-Privacy-Rule.pdf; Brief of Amicus Curiae EPIC, and Legal Scholars, in Support of Petitioners, *Sorrell v. IMS Health Inc*., 564 U.S. 552 (2011), https://epic.org/amicus/sorrell/EPIC_amicus_Sorrell_final.pdf; Comments of EPIC to Federal Trade Commission, Health Breach Notification Rulemaking, Project. No. R911002 (Jun. 1, 2009), https://www.epic.org/apa/comments/Comments_on_FTC_EHR-EPIC.pdf.

[4] 86 Fed. Reg. 6470.

[5] *Id*.

providers' Application Programming Interfaces (API). The proposed rule is in line with the 2016 Application Programming Interface (API) Task Force Recommendations, which established a solid framework for providing patients better access to their own healthcare information.[6]

However, HHS should go further to ensure that identity verification is not a barrier for patients to accessing their own information. Identity verification should be streamlined through the covered entities' online portals and limited to the minimum necessary information securely verify identity. EPIC urges HHS to develop more detailed guidance for identity verification procedures.

II. Care coordination and case management can be improved without diminishing privacy rights.

Several of HHS's proposals would limit patients' privacy rights in case management and care coordination scenarios. While case management and care coordination are an important part of any healthcare system, stripping patients of the right to decide how their information is handled will not improve these systems. HHS should instead adopt rules that empower patients in their own care coordination and prioritize individual control and meaningful consent. EPIC's responses to the specific case management and care coordination proposals are detailed below.

a. Part III C - Amending the Definition of Health Care Operations To Clarify the Scope of Care Coordination and Case Management (45 CFR 160.103).

EPIC opposes the proposed amendment to the definition of Health Care Operations in 45 CFR 160.103. Any amendment should explicitly exempt case management and care coordination from the definition. As written, HHS's proposed language would only slightly clarify the current text by replacing ambiguous commas with semi-colons.[7] However, the proposed text would cut patients

[6] Application Programming Interface (API) Task Force Recommendations (May 12, 2016), https://www.healthit.gov/sites/default/files/facas/HITJC_APITF_Recommendations.pdf.

[7] HHS's proposed text for § 164.501, "population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment."

out of decisions regarding their PHI, even when care coordination and case management activities are "focused on particular individuals".[8] HHS can do more to improve communication between providers than simply clarifying the grammar in an overly broad list.

This proposal cuts against the consensus definition of care coordination, which explicitly involves the patient in care coordination decisions.[9] While disclosure of some PHI is a barrier to effective care coordination, the type of disclosure required involves direct contact (e.g. conversations) between various members of a patient's care team.[10] Patients struggle to understand even the basic roles of various providers.[11] This problem is best solved by further involving the patient in their care coordination. By lowering the standard for disclosing PHI in the care coordination context, HHS is not incentivizing care coordinators and other healthcare providers to involve patients in the process. Instead, patients are denied another opportunity to understand how their information is being used, make informed decisions as to who can access that information, and in the process learn more about their care and the interaction between various care providers.

---

[8] 86 Fed. Reg. 6472.

[9] Ellen Schultz and Kathryn McDonald, *What is care coordination?*, 17 Int. J. Care Coordination at 19 (2014), https://www.researchgate.net/profile/Kathryn-Mcdonald-4/publication/280218337_What_is_care_coordination/links/562a76c808ae04c2aeb1a826/What-is-care-coordination.pdf ("Care coordination is 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 ser- vices. Organizing care involves the marshalling of personnel and other resources needed to carry out all required patient care activities, and is often managed by the exchange of information among participants responsible for different aspects of care").

[10] *See e.g.*, Christine Jones et. al, *A Failure to Communicate: A Qualitative Exploration of Care Coordination Between Hospitalists and Primary Care Providers Around Patient Hospitalizations*, 30 J. Gen. Internal Med. 417-424 (2015), https://link.springer.com/article/10.1007/s11606-014-3056-x? ("Hospitalists and PCPs were found to encounter similar care coordination challenges, including (1) lack of time, (2) difficulty reaching other clinicians, (3) lack of personal relationships with other clinicians, (4) lack of information feedback loops, (5) medication list discrepancies, and (6) lack of clarity regarding accountability for pending tests and home health.");

[11] *See e.g.*, Jennifer Walsh et. al, *What are the current barriers to effective cancer care coordination? A qualitative study*, 10 BMC Health Services Research 132 (2010), https://link.springer.com/article/10.1186/1472-6963-10-132 (finding that several patients, "acknowledged confusion about the roles and responsibilities of the different members of the health care team involved in their care" and that confusion increased with more complex care situations, where case management is most important).

b. Part III D - Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-Level Care Coordination and Case Management (45 CFR 164.502(b)).

EPIC opposes the HHS proposal to lift the "minimum necessary requirement" for disclosing PHI to health plans and covered health care providers.[12] Removing this requirement would open up new flows of data without patient consent, transparency, or practical accountability. Decisions about information sharing for care coordination and case management should be made in concert with patients, and should remain limited to protect patients from the risk of data breaches.

Data breaches are a constant threat across the healthcare industry and pose a substantial risk to patients. The number of healthcare data breaches rose 55% in 2020, to 599 breaches affecting more than 26 million people.[13] Hacking and IT security incidents are the most common causes of data breach.[14] Over the last 10 years more than 3,700 major data breaches were reported to HHS' Office of Civil Rights, leading to 268,189,693 health records exposed.[15] That amounts to over 80 percent of the U.S. population. Healthcare providers have also increasingly become targets of ransomware attacks because "patient care facilities are a category that is uniquely poorly positioned to tolerate network downtime."[16] And medical records are at an especially high risk because they are extremely valuable. A single medical record can be worth as much as $150 on the dark web.[17] There are already substantial risks of data breach in the healthcare industry, and HHS should take particular care to consider these risks when promulgating HIPAA rules.

---

[12] 86 Fed. Reg. 6474.
[13] Healthcare Breach Report 2021: Hacking and IT Incidents on the Rise, bitglass (Feb. 2021), https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q1HealthcareBreachReport2021.pdf.
[14] *Id*.
[15] Healthcare Data Breach Statistics, HIPAA Journal (*last accessed* May 5, 2021), https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[16] Scott Ikeda, *Rise in Healthcare Data Breaches Driven by Ransomware Attacks*, CPO Mag. (Mar. 18, 2021) https://www.cpomagazine.com/cyber-security/rise-in-healthcare-data-breaches-driven-by-ransomware-attacks/.
[17] *Id*.

Minimizing data transfers can mitigate the impact of data breaches by reducing the amount of patient information exposed in any single breach. The more often PHI is stored with multiple organizations, the higher the risk of a data breach exposing that information. Removing the "minimum necessary standard" will increase the risk and severity of data breaches without providing any benefit to patients.

c. Part III E - Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations (45 CFR 164.506).

EPIC opposes the HHS proposal to permit non-consensual disclosures of PHI to "social services agencies, community-based organizations, HCBS providers, and other similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management."[18] Many of these third parties are not healthcare providers and are often not subject to HIPAA rules; these third parties could include for-profit Home and Community Based Services (HCBS) providers. EPIC opposes non-consensual discloses of PHI outside emergency situations. Non-consensual disclosures of PHI risks alienating vulnerable patients and magnify risks of data breach, sale, or misuse of PHI as it flows to non-HIPAA compliant entities.

For individuals receiving social services like housing assistance, the proposed rule will expand the risk of data breach and may serve as a barrier to patients obtaining necessary services. Any non-consensual disclosure of PHI is a breach of the patient's trust, even if the Privacy Rule permits it. For individuals experiencing homelessness or in need of other aid, breaches of trust can lead to lower engagement or care avoidance, patients choosing not to receive necessary care.[19] In a study on transitioning homeless individuals with mental illness to stable housing, providers who

[18] 85 Fed. Reg. 6476.
[19] Fang-Pei Chen and Lydia Ogden, *A Working Relationship Model That Reduces Homelessness Among People With Mental Illness*, 22 Qualitative Health Res. 373-383 (Sept. 2, 2011), https://journals.sagepub.com/doi/10.1177/1049732311421180.

maintained "nonauthoritative" and "humanistic" relationships that respected patient autonomy generated more interest in long term stable housing.[20] Obtaining consent is a key element in recognizing and respecting autonomy. HHS risks further alienating vulnerable populations by encouraging non-consensual data transfers. The proposed runs contrary to the advice of experts by reducing patient autonomy and allowing providers to disclose sensitive information without consulting patients.

The proposed rule would also magnify the risk of data sale and data breach by authorizing non-consensual transfers to a wide variety of entities, some not subject to HIPAA requirements. Health information is now a major source of revenue for data brokers; hospitals executives report being "flooded" with requests for access to bulk health data.[21] Health data brokerage is now a multi-billion-dollar industry and it shows no sign of slowing down.[22] In this context, new flows of PHI should be carefully scrutinized to avoid monetization of patient data. Similarly, the substantial risk of data breach requires minimizing, not opening, data flows to protect patients. HHS should not permit non-consensual disclosure to third-parties in the name of care coordination.

d. Part III F - Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances (45 CFR 164.502 and 164.510-514).

EPIC opposes HHS's proposal to amend five sections of the Privacy Rule to replace the current "exercise of professional judgement" standard with a "good faith belief standard" for individuals experiencing Substance Use Disorder (SUD), Serious Mental Illness (SMI), and Emergency Circumstances.[23] The Department's proposal does not give sufficient weight to patients'

[20] *Id*.
[21] Christina Farr, *Hospital execs say they are getting flooded with requests for your health data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.
[22] Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Sci. Am. (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.
[23] 86 Fed. Reg. 6480-81.

serious privacy concerns, particularly with respect to substance use and mental illness, two highly-stigmatized conditions. Lowering the standard for disclosing PHI of individuals with SUD and SMI would create serious risks of harm and increase barriers to care. Patients with highly-stigmatized conditions need the highest levels of privacy protections to encourage disclosure of those conditions and protect patients from harm.

HHS's proposed guidance would permit licensed health care professionals, including front desk staff, to disclose PHI based on a "good faith belief" even when such a belief did not conform with the staff member's professional training. The upshot is that PHI can be revealed by care providers with a limited understanding of the patients' situation. To draw this out, consider HHS's proposed example,

> the proposed change would permit a covered health care provider to disclose PHI of an un-emancipated minor experiencing SUD in a state or jurisdiction where applicable law does not treat the minor's parent as a personal representative, when the provider believes that disclosing information to the parent could improve the care and treatment of the minor.[24]

The front-desk provider at a clinic then would need no more than the unsupported belief that disclosing a patient's PHI would improve care and treatment, even if that provider has no knowledge of the patient's family situation. For a minor at risk of abuse, revealing details such as the upcoming schedule of appointments could lead to a parent denying the minor access to treatment.

If a provider can disclose details of a minor's substance abuse disorder or mental illness without enquiring carefully into the patients' situation, providers will create scenarios where disclosing PHI leads to "discrimination, abuse, and retaliation" against patients.[25] HHS is well-aware of the risks involved, noting in the NPRM that "patients or privacy advocacy groups almost

[24] 86 Fed. Reg. 6481.
[25] 86 Fed. Reg. 6480.

universally opposed modifying the Privacy Rule to expand permitted disclosures of information related to SMI and opioid use disorder or other SUDs."[26] Yet HHS is cavalier about the risks the NPRM creates, "The Department assumes that health care providers would incorporate relevant concerns about an individual's risk of abuse as a key factor in whether a disclosure of PHI is in an individual's best interest."[27] HHS should base decisions regarding patient well-being on more than mere assumptions. HHS should not permit non-consensual disclosure of PHI for patients with SUDs or SMIs. The "good faith belief" standard should not replace a high "professional judgement" standard in any context.

Conclusion

EPIC urges the Department to adopt HIPAA Privacy Rule modifications that prioritize patient privacy and strengthen meaningful consent requirements. The Department should not lower the standard for disclosing PHI without patient consent, and should be especially careful to protect patients with mental illness and substance abuse disorders. HHS can protect patients and promote better quality care by involving patients in decisions regarding their PHI. Opening up end-runs around consent poses numerous dangers to patients including data breach, loss of trust in healthcare institutions, and increased stigmatization of vulnerable populations.

Respectfully Submitted,

Jake Wiener
Jake Wiener
EPIC Law Fellow

[26] *Id.*
[27] 86 Fed. Reg. 6841.