Comments of the World Privacy Forum to the U.S. Department of Health and Human Services, Office for Civil Rights Regarding Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement NPRM, RIN 0945– AA00

Via OCRprivacy@hhs.gov

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement NPRM, RIN 0945– AA00
Hubert H. Humphrey Building
Room 509F,
200 Independence Avenue SW,
Washington, DC 20201

May 6, 2021

The World Privacy Forum welcomes this opportunity to offer comments on the *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement*, 86 Federal Register 5446, January 21, 2021, https://www.govinfo.gov/content/pkg/FR-2021-01-21/pdf/2020-27157.pdf. The comment period for this NPRM was extended on March 10, 2021 to May 6, 2021. See https://www.federalregister.gov/documents/2021/03/10/2021-05021/modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care-and .

The World Privacy Forum (WPF) is a nonprofit, non-partisan 501(c)(3) public interest research group. WPF focuses on multiple aspects of privacy, with health privacy being among our key areas of work. We publish a large body of health privacy information, including guides to HIPAA; reports and FAQs for victims of medical identity theft; and materials on genetic privacy,

precision medicine, electronic health records, and more.[1] We testify before Congress and federal agencies, and we regularly submit comments on HIPAA and related regulations. WPF participates in the WHO and serves on its data governance workgroup. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and comments at http://www.worldprivacyforum.org.

In general, we find much to support in the NPRM. However, there are sections of the NPRM that repeal key privacy provisions of HIPAA, and weaken others. Patients' access to their health records is an essential element of privacy, and actions that will simplify patients' access are generally welcome. However, not all of those actions are uniformly positive, and there can be negative consequences for patients and for the health care system in general.

Some of the tradeoffs here are especially difficult because worthy goals raise conflicts and present sharp dilemmas, which we discuss in some detail in these comments. We note that some of the proposals in the NPRM, if allowed to move forward, would have the effect of repealing key privacy provisions of HIPAA, particularly § 164.510(b). We discuss this provision in more detail below. At the close of these comments you will find specific recommendations we offer to mitigate some of the risks that this NPRM raises. Some of the risks, however, need to be mitigated by HHS rolling back some of the problematic provisions in this NPRM.

Part I. General Comments

1. Access

The NPRM proposes a series of changes to improve patient access to their records. We support those provisions that:

1. Allow greater in-person inspection;
2. shorten response time to requests;
3. clarify the form and format of responses;
4. reduce the identification verification requirement;
5. require health care providers to respond to requests from other providers;
6. all provisions relating to fees, fee schedules, and fee estimates.

We would also support a requirement that mandates that all electronic record disclosures to a patient be without any charge at all. The costs of providing a copy of an electronic record are trivial, and the costs of collecting fees and making decisions about those unable to pay will be greater than any allowable direct costs.

---

[1] See World Privacy Forum, A Patient's Guide to HIPAA, https://www.worldprivacyforum.org/2019/03/hipaa/; see also our Health Category page for additional materials https://www.worldprivacyforum.org/category/health-privacy/.

We recommend that the Department take fees off the table entirely for patient access.

2. Care Coordination and the Loss of the Minimum Necessary Exception

The proposed rule would amend the definition of *health care operations* to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management that constitutes health care operations. In this section, we discuss the reasons why the proposed care coordination language is deleterious and needs to be removed from the NPRM.

A. WPF disagrees with the proposal to remove patient consent for care coordination and case management

The proposed change regarding care coordination and consent is troublesome for several important reasons. First, it is another step down the road of removing patient consent from all use and disclosure decisions. The existing rule already does that to a tremendous extent, although we agree that not all of those choices are necessarily bad ones. However, there is still a role for patient consent even if it is inconvenient for the health care system to obtain consent. As one moves further and further away from direct patient care, the justification for evading consent grows weaker. Poorly defined care coordination and case management activities are excellent examples of consent exceptions that are not justified. When one analyzes the Department's justification, it is based on administrative convenience, not patient or other necessity.

B. HHS has not defined care coordination or case management

Second, the Department itself cannot define either *care coordination* or *case management*, and it admitted that in the NPRM:

> Although neither care coordination nor case management has a precise, commonly agreed upon definition, both refer broadly to a set of activities aimed at promoting cooperation among members of an individual's health care delivery team, including family members, caregivers, and community based organizations. (page 6449)

If this language is incorporated into the rule, the result will be that anyone in a health care setting, professional or otherwise, can decide to disclose a patient's record – without the patient's consent and over the patient's express objection – to virtually anyone who claims they are conducting *care coordination*. Teacher? Landlord? Grocery store shopper? Auto mechanic? Uber or Lyft driver? With the right spin, any of these activities could be construed as care coordination. Asking for patient consent in these circumstances would be messy. But removing the patient consent in the name of *care coordination* is in the long run much messier, and will create a lot of fresh problems.

The proposed change in regards to the care coordination and consent language is deleterious enough that we have to wonder why HHS decided that it was appropriate, and how HHS could justify this change on a fully-researched, factual basis, inclusive of patient experiences and actual fact patterns.

We understand that certain parts of the health care sector maintains that it isn't worth the trouble to ask patients for consent. Patients believe otherwise, however, and for good reason. At a time when patients are already smarting from having to disclose personal health information more widely than is usual due to the pandemic, this proposed language will add fuel to the fire of patient mistrust in the health care sector at a challenging moment in time when more, not less, trust is needed.

No matter how strong the justification may look on paper, in reality and practice this particular language is associated with increased risks for the patient, and could lead to meaningful privacy problems for patients, particularly for victims of domestic violence and other crimes, where information in the wrong hands can pose meaningful safety risks. Safety risks we note that are all too real, and do not suffer from being just theoretical privacy risks. What the Department chooses to do with this language will have real consequences for patients, particularly the most vulnerable.

C. The proposed changes to care coordination language will in effect repeal § 164.510 (b) HIPAA privacy protections

Third, other existing provisions of HIPAA allow a patient to object to sharing with family members, but this new provision says that patient choices are not relevant here. The effect is to *undermine* one of the few places in the existing rule that recognizes patient choice during the routine provision of health care.

The proposed language says, in essence, that **a provider can ignore a patient's objection to sharing with a family member that § 164.510(b) protects**. If this provision proceeds as is, the Department needs to explain how these conflicting provisions should be reconciled. Otherwise, the effect will be to repeal § 164.510(b). This would be a terrible outcome for patient privacy, especially at a time when patients are more concerned than ever about expanded flows of their health information.

D. No requirement that care coordination disclosures be made by a health care professional

Fourth, there is no requirement here that the decision to make these disclosures be made by a health care professional. Any employee of a health care provider, from the treating physician to the orderly who cleans the room, has the same authority under this provision to make these undefined disclosures.

We urge the Department to drop these changes entirely. Alternatively, if the Department is unwilling to drop the changes entirely, we suggest that the Department add procedural protections for patient privacy. Procedures offer a standard way of dealing with the inability to write clear standards that define and direct actions. We offer three ideas:

1. Require a judgment of a **health care professional** that the disclosure is necessary (or appropriate) for patient care;
2. require a **professional judgment that the disclosure is in the interest of the patient and likely to result in better outcome for the patient**;
3. direct each health care provider to **designate by role all personnel authorized to make these disclosures** and also designate those who are not authorized.

The problem the proposed language creates is made even worse by excepting care coordination or case management disclosures from the minimum necessary rule. The effect is that anyone can disclose anything and *everything* under a vague standard. As proposed, there is no need for a physician or any professional judgment. Anyone can just hit the SHARE button and send an entire patient record to some other organization not directly involved in treating the patient whether that organization needs the entire record or not. An exception from the minimum necessary rule just compounds the problem created in the first place.

The Department worked hard to stop the casual sharing of entire patient records. This is no time to stop. We urge the Department to reject this minimum necessary exception.

3. "Good Faith Belief" is a significant weakening of the existing HIPAA standard; WPF strongly opposes the proposed change

The Department proposes to replace the privacy standard that permits covered entities to make certain uses and disclosures of PHI based on *professional judgment*. The proposed replacement is a standard permitting such uses or disclosures based on a covered entity's "good faith belief" that the use or disclosure is in the best interests of the individual. The proposed standard is even more permissive than it appears upon first glance. This is because it would presume a covered entity's good faith, but this presumption could be overcome with evidence of bad faith.

The World Privacy Forum opposes this change. We recognize the appeals made by families of individuals with substance abuse disorders, which we have sympathy for. However, the change appears to be guilty of "*doing something-ism"* rather than solving a clearly defined problem with a clearly defined response. It is an unfortunate example how edge cases can make bad law.

The Department recognizes that patients and patient advocates are "almost universally opposed" to modifying the rule in this regard (page 6480). That opposition is telling. The Department also recognizes that the privacy rule already allows many of the disclosures at issue here are already allowed by the privacy rule. If covered entities are unwilling to make allowable disclosures, it

may not matter what the standard is. They can refuse just the same under a weaker standard. Overly cautious lawyers are likely to be just as overly cautious whatever the standard.

For example, we are aware that some covered entities still refuse to disclose PHI to a treating physician of another institution without patient consent, even though those disclosures are *expressly* allowed by the rule without any standard at all. There are few practical remedies that will overcome narrow-minded lawyers. Mandates and sanctions will not work, and no rule could be specific enough to accomplish the purpose, overcome the definitional challenges, and address the ethical objections.

What is most troublesome here is that the Department proposes to change the rule covering a large class of allowable disclosures while those seeking adjustment here only represent a small fraction of the affected universe. In effect, the proposal proves too much. This proposal removes existing protections that appear to be working without objection in other circumstances.

The proposed change cannot assure those who seek the change that they will obtain the outcome they seek, but it will certainly undermine meaningful privacy interests of everyone else. In short, the proposal will make many patients worse off while not guaranteeing that any patients will benefit.

Further, for that large class of other patients affected by the proposed change, it would be nearly impossible to make a case that a provider disclosed a record improperly under the good faith standard. The burden of proving bad faith and the burden of going forward would fall entirely on the patient. The only source of information belongs to the health care provider, who would surely treat the information as prepared in anticipation of litigation. Most patients would have no chance of success because the rule does not require that a provider adequately document any disclosure made under the good faith standard.

WPF joins the overwhelming number of patients and patient advocates and we strongly oppose this change. WPF opposes the NPRM language because it may not help any patients at all, but it will surely harm the privacy interests of almost all others. If the Department is determined to proceed, despite strong public objections from patient advocates, patients, and more, we suggest that the change **apply only in substance abuse matters**. The right principle is *do not harm*. Do not undermine everyone's privacy interest to assist a narrow class. We recognize the seriousness of the substance abuse problem, but the proposal will not help, no matter how well intentioned it is.

4. Proposed changes to rules of disclosure of PHI to avert threats to health or safety is too permissive

The Department proposes to expand the ability of covered entities to disclose PHI to avert a threat to health or safety when a harm is "serious and reasonably foreseeable," instead of the current stricter standard which requires a "serious and imminent" threat to health or safety.

This is a troublesome issue, and we understand the Department's search for a good faith solution. Nevertheless, we think that the proposed standard is far too permissive. The new standard appears to allow disclosures by covered entities based on these types of judgments:

1. If the patient continues to eat junk food, the patient may have serious adverse health effects in five years;
2. if the patient does not get more exercise, the patient may experience a heart attack or stroke in the future;
3. if the patient does not lose weight, the patient may die prematurely at some time in the future.

We worry that if the constraints of the current policy are lifted, then medical bureaucrats of all stripes could feel justified to take steps to stop patients from living their lives as the patients see fit. We recognize the benefits of better diets, exercise, and weight loss. Patients – all of us – face hard choices here. However, "emergency" interventions by health plans or others on the basis of a *serious and reasonably foreseeable* harm standard could produce unexpected and unwelcome actions, as well as unintended consequences.

All manner of well-intended interventions could occur at grocery stores and other retailers, at the patient's place of work, in travel scenarios, and with the patient's friends and family members. Based on the proposed language, several scenarios would be possible.

- If a covered entity were to circulate a list of chronically ill patients to bars and restaurants on the grounds that serving alcohol to them would present a *serious and reasonably foreseeable threat* to their health, it would be allowable under the proposed rule.

- Providers and health plans (for example, Medicare) could use the new authority to seek to force patients to follow recommended health standards whether the patients want to or not. One can readily imagine just-in-time, geolocation-based notifications to patients' mobile devices noting that a patient should not be ordering certain menu items, purchasing certain items, or engaging in any manner of other activities.

It would all be in the interest of preventing "foreseeable harm" that would occur in five hours, five weeks, or could even encompass warnings that prevent harms that could occur in ten years' time. Even if everyone were truly motivated by what they see as the patient's best interests, patients are not likely to agree.

We recognize the need for flexibility in making disclosures to avert genuine and imminent health and safety threats. We are not convinced that the requirement of *imminence* is that serious of a barrier. In the end, what is needed for these types of disclosures is **reasoned judgment by a covered entity under all of the circumstances**. It is hard to write a few words to direct that judgment in myriad circumstances.

We suggest that the Department consider using the notion of *emergency circumstances* as an alternative to *imminence*. There is a need for some restraint so that the authority for health and safety disclosures is not used routinely to address longer-term health care issues affecting patients because the standard is too weak and the authority is unbounded. The class of disclosures allowed under the health and safety standard must not be allowed to be routine. It should be based on some type of unusual or extraordinary circumstances, and the proposed change lacks that constraint. A rule that is so unconstrained that it might allow a provider or plan to have overbroad reach to object in real time to patients' choices in eating, shopping, or more is just too broad.

5. Changes in Patient Acknowledgement for Notice of Privacy Practices (NPP)

The Department proposes to eliminate the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP).

The World Privacy Forum supports this proposal. The requirement was a good idea, but in practice it has proven to be a "click-through" situation that often defeats the purpose of the exercise. In practice, the collection of a signature from a patient became an act wholly separated from distribution of an NPP. It did little to improve patient understanding about privacy.

A related proposal would improve patient understanding of useful information in the NPP. We support those changes as well, but with some qualifications.

First, the rule requires that the header on an NPP be in ALL CAPS. We observe that text in all caps is harder for many people to read and understand. The Department may want to ask reading experts for views here, but we think that text in ALL CAPS should not be required.

Second, we have significant concerns about how the Department is making it easy for patients to share information with third parties — for e.g., data brokers, social media sites, and others who fall outside the scope of HIPAA protections and outside the scope of any privacy law at all. We have lengthy comments on this subject that we include in part II below.

Part II. The Dilemma Posed by Third-Party Access to EHRs

In this NPRM and in others, the Department is moving step-by-step to support patient access to records in a way that also allows third parties (e.g., social media companies, health apps, fitness apps, even data brokers, among many others) to serve as hosts. These actions by the Department present a pressing dilemma. On the one hand, both the Department and the World Privacy Forum agree that patients should have a broad right of access to their health records. That access is

required by law, and we support that law.[2] The right of an individual to see and have a copy of their records is a fundamental principle of privacy that dates back to the origins of modern privacy policy. The report of the (HEW) Secretary's Advisory Committee on Automated Personal Data Systems, one of the most important policy documents in the history of privacy policy, concluded that individual access to their records is a major element of fundamental Fair Information Practices (FIPs).[3] FIPs are at the core of nearly all privacy legislation all around the world, including the HIPAA health privacy rule.[4]

On the other hand, in today's environment, providing patients with "one click" complete electronic copies of their health records will have significant deleterious effects on patients, their privacy, the practice of medicine, the cost of health care, and other institutions and policy objectives. In one sentence, the problem is that EHRs made readily available to patients will end up in the hand of third parties, including banks, data brokers, marketers, merchants, foreign governments, and an untold number of websites. Sadly, patient records will also be prized fodder for fraudsters, and we expect to see pronounced efforts over time to acquire and utilize patient records by fraudsters. Even for good actors and companies or educational institutions who are working to access records for legitimate purposes, many of those who currently want to be users of patient records are entirely unregulated for patient privacy in the United States.

We emphasize that notwithstanding these unwelcome effects, we still fully support patient access to records in whole and in useful electronic formats. These comments address more about the problems and offer some thoughts about how to proceed in light of the dilemma.

It appears to us that the Department is fully aware of the dilemma that set out here. The Department is implementing a variety of legislatively directed mandates that give rise to the problem. We acknowledge that the Department is proceeding in good faith to carry out those mandates. One cause of the problem may be a lack of congressional attention to privacy and a lack of awareness of the consequences of some of its directions. This is not the first time that congressional actions failed to see the broad ramifications of legislation. Indeed, the history of EHRs is filled with other examples.

We have some suggestions for addressing the problems, but we admit that we do not have a comprehensive solution.

---

[2] WPF supports even broader access by patient to their records than the HIPAA privacy rule allows. We would narrow or eliminate some of the provisions that allow a covered entity to withhold records from a patient. Since the rulemaking does not raise that issue, we will not comment further on it. This is just a marker.

[3]Records, Computers and the Rights of Citizens (1973), http://epic.org/privacy/hew1973report/default.html.

[4]For a history of Fair Information Practices, see Robert Gellman, FAIR INFORMATION PRACTICES: A Basic History (last version 2017), http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

1. The Modern Health Data Environment: Complex health data ecosystems and implications for the NPRM approach to third parties

Today's health data ecosystems are incredibly complex. The complexity is well-known to health practitioners. These ecosystems have porous edges in many important respects — covered entities under HIPAA no longer hold all health data that is generated. There is a lot of pressure from the inside of the HIPAA-covered ecosystem to share health data within the system, and also outside of the system, with boundaries and rules in place. But that is not the end of it - there is also increasing pressure for health providers to utilize broader data sets than just PHI held under HIPAA in order to gain a broader context for a patient's health, or for analyzing disease patterns in a community, city, state, or nation.

WPF has been researching and writing about health data and health privacy for two decades. During this time, we have found that health care providers take HIPAA seriously. We have not found health care providers knowingly selling lists of patient data, excepting the truly bad actors, such as medical identity thieves, which is a separate issue. However, the protections of HIPAA that have in the past prevented ecosystem leakage, stand to be weakened by the NPRM proposal. The World Privacy Forum is concerned about the extensive implications of opening up complete patient medical records to "one click" transmission to non-health related third parties outside of the health care system.

We understand the deep trendlines in health data ecosystems; that is, the ecosystems are becoming more porous and allowing for more and easier sharing. However, we also understand the deep trendlines of rules and policies that create unhealthy data ecosystems, and some of the proposals HHS has put forward will indeed result in problems for health data ecosystems and patients. We have written in some detail about the key problems relevant to this NPRM.

A. Patients and EHRs

What will happen when patients have ready access to their EHRs? We believe this access is critically important, and we support better access. We do not deny these benefits. We note in passing that over the past several decades, the broad benefits of EHRs have been widely predicted and touted. The reality, as the Department is already fully aware, has been far different.

The promised benefits of administrative simplification were not realized in large part. The spread of EHRs changed the way that physicians practice medicine, as physicians spend their seven-minute visits with patients mostly in front of computer screens rather than actually examining or

even looking at patients. EHRs became tools for upcoding, and EHR systems became non-interoperable because of the proprietary interests of EHR vendors.[5]

The new prohibitions against information blocking and supporting interoperability are, like the push for EHRs, intended for good reasons. The consequence of these changes could potentially result in positive changes for patient access, but because of how the rule has been proposed, the changes also result in the expansion of patient records going to third parties. WPF supports patient access. We are troubled, though, by the HHS proposal facilitating patient records going to non-health third parties.

We predict that the 3rd party change may make things worse for patients and providers in unpredictable and systemically deleterious ways. We are not against improved information technology, and we recognize that the health sector, broadly speaking, has lagged behind here. We merely observe that predictions about the benefits, process, and consequences of adding technology to health care have been consistently off the mark.

We note that in 2005, there was a strong push to move patients to EHRs, along with a strong push to develop a National Health Information Network (NHIN).[6] The World Privacy Forum testified before the NCVHS regarding the proposed National Health Information Network and EHRs, focusing on the risks of such a network, and the risks of EHRs.[7] To illustrate the risks, for the first time in a public hearing, we testified about the issue of **medical identity theft** as a risk factor in EHRs and the NHIN.[8]

WPF documented the facts of medical identity theft in 2006 when we published the first known report documenting medical identity theft modus operandi, harms, protocols, and multiple cases of the crime and impacts. Medical identity theft results from the fraudulent use of patient health records in ways that were - and still are — profoundly harmful to patients. WPF saw this problem because of the data flows that already exist in electronic health records systems and health data ecosystems. Some of those data flows can be exploited by bad actors. Now, in the

---

[5]See generally, Fred Schulte & Erika Fry, Kaiser Health News, Death By 1,000 Clicks: Where Electronic Health Records Went Wrong (Mar. 18, 2019), https://khn.org/news/death-by-a-thousand-clicks/; Fred Schulte & Erika Fry, Kaiser Health News, FDA Chief Calls For Stricter Scrutiny Of Electronic Health Records (Mar. 21, 2019), https://khn.org/news/fda-chief-calls-for-stricter-scrutiny-of-electronic-health-records/.

[6] National Health Information Network Timeline, World Privacy Forum. Available at: https://www.worldprivacyforum.org/2009/02/report-nhin-timeline-documenting-the-history-and-development-of-the-national-health-information-network/

[7] Pam Dixon, Testimony: *Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environments,* NCVHS, August 16, 2005. Available at: https://www.worldprivacyforum.org/2005/08/public-comments-testimony-before-the-national-committee-on-vital-and-health-statistics-ncvhs-subcommittee-on-privacy-and-confidentiality/

[8] Id.

same way, WPF sees serious systemic problems arising from this HHS proposal for patient sharing of full patient records with non-health related third parties.

We want to address some key ways that EHRs shared with patients will pour out into the hands of third parties.

- **Data Breach.** the Department knows about the volume of data breaches from HIPAA covered entities.[9] In most cases, these breaches occur despite security measures required by the HIPAA security rules. When patients download their EHRs on their cellphones, tablets, and home computers, those EHRs will be much more vulnerable to being breached because securing home and person devices is exceptionally challenging. Those who steal passwords, account numbers, and financial data will be just as happy to steal EHRs from patients. The market for health data is well-established already, and there is regrettably an underground market, too.[10] Patients with EHRs on their devices could find themselves with additional risks from thieves and from foreign governments that may seek to collect and exploit health data on Americans for purposes that are at odds with American interests.

- **Medical Identity Theft.** The epidemic of medical ID theft will mushroom with the greater circulation of EHRs outside of the health care system. Already, medical identity theft occurs in every state in the US.[11] Medical ID theft occurs today even with limited available of health information. A patient name, account number, and Medicare or insurance number is more than enough to allow crooks to profit.[12] With full EHRs obtained legitimately or fraudulently from patients, medical ID theft will skyrocket. Data indicate that medical identity theft is already growing steadily each year in the US.[13] Based on the information available, it is highly likely that data brokers and others will be able to acquire, compile, analyze, and sell identifiable patient data with details of insurance coverage and other detailed information, such as insurance identification numbers. We are concerned that fake health clinics —

---

[9] Interactive Medical Data Breach Map, World Privacy Forum. Available at: https://www.worldprivacyforum.org/2016/09/2016-breach-interactive/

[10] See, e.g., Chris Bing, Cyberscoop, Abundance of stolen health care records on dark web is causing a price collapse (Oct. 24, 2016), https://www.cyberscoop.com/dark-web-health-records-price-dropping/; Jennifer Schlesinger & Andrea Day, CNBC, Dark Web is fertile ground for stolen medical records (Mar. 11, 2016), https://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html.

[11] Pam Dixon, The Geography of Medical ID Theft, December 2017, World Privacy Forum. https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/

[12] Pam Dixon, Medical Identity Theft: The information crime that can kill you, World Privacy Forum, May 2006. https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/ .

[13] Pam Dixon, The Geography of Medical ID Theft, December 2017, World Privacy Forum. https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/

such as those we documented in our Medical Identity Theft report and those that are well-known to CMS fraud investigation units — will be able to scour this new source of EHRs to find justification to bill for expensive tests and procedures fully justified by a patient's actual documented health condition. Patients affected by this crime will find it even harder to keep up with and correct erroneous additions to their EHRs, and the erroneous information will follow them around because HIPAA provides inadequate remedies for patients seeking to recover from medical ID theft.[14]

- Malpractice. Lawyers who bring malpractice suits on behalf of patients will find EHRs outside of HIPAA to be a vast new resource. They will be able to scan records electronically looking for possible causes of action against, physicians, hospitals, pharmaceutical and device manufacturers, and others. We can already hear the late-night television ads offering the hope that your health records will point the way to a multi-million-dollar malpractice judgment. Just sign the consent form and wait to see if money will come your way.

The uses of these records for highly targeted advertising are so obvious that we will not stop to dwell on them other than to observe that personally targeted health ads based on an actual diagnosis will become much more ubiquitous and much more focused than they are today.

2. Methods of access

It is likely that there will be several ways for a patient to use an EHR. Some may be able to access and use an EHR hosted by a HIPAA-covered entity on a website maintained by the covered entity. This may be the best of all possible worlds because patients will have access, the EHR will presumably be regularly updated by the covered entity, and the covered entity will be responsible for the security of the entire system. In our minds, this is ideal. Patients will still face new risks because the usual cast of fraudsters will seek to steal passwords and to use the passwords to access and perhaps download the entire EHR. However, using an EHR system hosted by a HIPAA-covered entity affords the provider the opportunity to educate patients about providing third party access, and to create a protective layer of information and interfaces around that decision point.

A second way for a patient to use an EHR is to download the EHR onto a personal computer or to a mobile phone. A record stored in either location will be more vulnerable to access by others. We are concerned that at some point in time, third parties will request access to EHR data routinely, along with the patient's contacts, location, and other information on the mobile phone. Once an EHR passes into the hands of a patient, the EHR falls outside of HIPAA so that any

[14] FAQ: Medical ID Theft: How to recover if you're a victim, and what to do if you are worried about becoming a victim, World Privacy Forum https://www.worldprivacyforum.org/2012/04/faq-victims-of-medical-id-theft/

downstream recipient (other than a covered entity) will be able to use the EHR without any HIPAA constraints.

A third way for a patient to use an EHR is to use a resource provided by a third party app or a website that offers to host the EHR. The data in EHRs will be so lucrative that sites and apps will line up to obtain access by hook or by crook.[15] EHRs stored in this fashion will also fall outside of the HIPAA protections.

In the Covid-19 era, there are now many third parties who might seek patient consent for EHR access. These now include travel-related companies such as airlines or cruise lines or hotels, seeking data for the spate of forthcoming "vaccine credentialing systems" such as the Digital Green Pass, which is but one of many initiatives in this area seeking to certify patient vaccination. Other entities that may want access to patient records include gyms, life insurers, schools, health practitioners not subject to HIPAA, state motor vehicle departments, immigration authorities in the United States and in other countries, countries that issue visa to travelers from the United States, and any institution with market power over individuals.

When and if EHRs become readily available to third parties, we predict that new start-ups will emerge to exploit the records, and most of these activities will not benefit patients or the health care system in any useful way. The average consumer will not stand a chance. Many of those who chose to download their EHRs will end up with their entire health records in the hands of multiple third parties. The records in the hands of these third parties will have little or – more likely no – legal privacy protections at all.

Most consumers will be unaware of these consequences. After a patient's health records end up in the hands of an unregulated party, that record will be used by marketers, junk mailers, quacks, fake supplement sellers, and more. [16]There is no time limit. The record will haunt the patient for the rest of their life, and for their heirs as well. There is no way under current law to stop unregulated actors or to retrieve the records they obtain with patient consent. Records that find their way to the dark web will be irretrievable lost forever beyond all hope of control.

We would suggest the possibility that EHRs could be exported to third countries and to actors there who are beyond the reach of American law and institutions. However, most other countries around the world have general purpose data protection laws that provide meaningful privacy rights to data subjects. The export of EHRs to evade restrictions here is, at present, undesirable

---

[15] See, e.g., Ed Cara, Gizmodo, Researchers Create Fake Profiles on 24 Health Apps and Learn Most Are Sharing Your Data (Mar. 21, 2019), https://gizmodo.com/researchers-create-fake-profiles-on-24-health-apps-and-1833474535.

[16] See, e.g., Natasha Singer & Katie Thomas, Drug Sites Upend Doctor-Patient Relations: 'It's Restaurant-Menu Medicine' (Apr. 2, 2019), https://www.nytimes.com/2019/04/02/technology/for-him-for-hers-get-roman.html.

because there are more privacy protections for consumer records almost everywhere else in the world than in the United States.

3. Costs

The fiscal cost of health care is not an issue the World Privacy Forum studies. However, we observe in passing that many of the consequences of patient access and the spread of patient data across multiple data ecosystems (data brokering, advertising, and potentially many others) are likely to bring increased costs for the health care systems overall. We also note that the costs of fraud and misinformation could mount to surprising levels after patients' EHRs become widely available by patients' consent to third parties. After this point, there is no telling how the ingenuity of fraudsters — from fake supplement manufacturers to fraudulent health clinics, and assorted others will expand to soak up more money from the health care system and from patients unable to distinguish truth from fantasy. This is a serious risk, and the proposal from HHS has not offered any mitigation for concerns of fraudulent requests for patient health care data, or uses of that data after acquiring it.

Here is one possible scenario. A patient has a blood test on Friday. The results are posted to the patients EHR and online portal on Saturday. The patient's EHR host (or other third party the patient has granted access to) obtains the results immediately upon posting based on the patient's previous authorization. The test results are normal, and the patient won't hear that from the provider until Monday or later. However, we can take just one element of the test to illustrate the problem. The blood test finds that the calcium level is 8.7. The normal range for that result is between 8.6 and 10.3. The result is normal. But to a marketer of dubious supplements, that test result is low, in fact, well below the average. We leave it to your imagination how that marketer might contact the patient with multiple, urgent messages that the patient needs to take immediate action to raise that calcium level. A clever marketer might compare the result to the previous blood test that showed a result of 8.9, suggesting that the calcium level is dropping like a rock. The marketer can promise next day delivery of calcium supplements.

We observe that greater accessibility to patient EHRs could create new opportunities to affect health care in other unwelcome ways. For example, a campaign against generic drugs might attract considerable funding (on a not-for-attribution basis, of course) from those with a vested interest in proprietary drugs. An advertising campaign targeting individuals using information from their EHRs has great potential to be successful enough, especially when the facts are not of any particular concern to true believers or to crooks. We note that anti-vaccination campaigns have met with success even though there is often no financial incentive to oppose vaccination. Those who can find a way to profit can inflict considerable harm on the health care system in general with actual patient information in their hands.

B. Ideas for Solving the Problems Created by Third Party Access to Patient Health Files

1. Federal Trade Commission involvement

The Federal Trade Commission has jurisdiction over many of the companies not covered by HIPAA that engage in the collection and sale of consumer health information. We urge HHS to hold a joint hearing or workshop with the FTC that examines the intersection between commercialization of patient health data, patient consent interfaces (including dark patterns that can trick patients into disclosing records), and the forthcoming free flow of patient records through multiple non-health data ecosystems.

The FTC does have limitations and cannot be expected to enforce away a bad regulation that allows unrestricted sharing. But working with the FTC to ensure there are state-of-the-art consent mechanisms, proper notice, and some form of FTC involvement could be helpful here.

2. HIPAA-covered entities should have a role in being able to refuse or restrict requests from non-health entities which could be harmful to patients

No matter how well-meaning the intent, HIPAA-covered entities will not be able to police how EHRs are accessed or used by third parties outside the domain of HIPAA. After patients click a tick box to release their records, the records will be in the hands of a third party. Covered entities are likely to view this as not their problem. If patients obtain their own EHRs and transfer the records to third parties, then covered entities will play no role at all in the activity. Even if a covered entity tries to limit release of an EHR to a third party in some circumstances, there will almost certainly be another covered entity willing to provide the records. When "Junk Mail America, Inc." contacts a hospital with signed authorizations from 5000 patients, the hospital has no grounds to contest the demand for records.

The World Privacy Forum suggests that the Department revisit 45 CFR § 164.524(c)(3)(ii). No covered entity should be able to impede direct demands from patients, patient's lawyers, or personal representatives, nor should there be barriers to the disclosure of health information to other health care providers. But covered entities need to have a way to restrict or refuse demands from any entity which could be harmful to patients. This could fall into myriad categories, some of which will shift and change with time.

We note here that apparently no consideration was given to victims of crime, including crimes of domestic violence. There are significant safety issues relating to the release of health records to third parties who have attempted to harm the patient in a criminal act. This is particularly true in domestic violence incidences. We also note that during the Covid-19 emergency, we have seen a significant uptick in problematic health information releases to unsafe third parties who are family members. This and other safety issues need to be addressed by HHS in a way that aligns with the protections already afforded in the Violence Against Women Act.

3. Self-regulation: *No*. Voluntary Consensus Standards: *Yes*.

WPF does not believe that "self regulation" should be an option here. Self-regulation has proven to be highly ineffective.[17] However, Voluntary Consensus Standards (which OMB has outlined in OMB Circular A-199 https://obamawhitehouse.archives.gov/omb/circulars_a119_a119fr) are fit for purpose here. VCS are already in use by HHS. The FDA utilizes Voluntary Consensus Standards to allow industry and other stakeholders to create VCS standards for medical devices, this in lieu of lengthy ANSII processes for standards. It has worked extremely well; see for example the 1,400 - plus medical devices standards created under voluntary consensus standards: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/results.cfm. The approach of utilizing one-sided, industry-only self-regulation without any direct and meaningful participation by consumer representatives and other stakeholders has consistently failed to protect consumers in any meaningful way. With the availability of voluntary consensus standards under OMB Circular A-119, this should be the only consensus mechanism considered.

4. Consumer education

Educating consumers about anything is a hard task. We do not oppose consumer education, but we have no great expectation that it will be as effective as it needs to be to provide adequate consumer protection. In a nutshell, there is too much competition to educate consumers about issues like blood pressure, nutrition, computer security, financial matters of all stripes, auto safety, and dozens of other important topics. The health care system does a poor job of educating patients about HIPAA. The World Privacy Forum has some experience here. We offer *A Patient's Guide to HIPAA*, [18] and we observe that even after 12 years of publication, there are few, if any, comparable guides for patients available anywhere. The notion that someone, somewhere will effectively educate patients about the real-world and quite meaningful consequences of sharing their EHRs with non-health third parties is, unfortunately, unlikely. What we try to do is provide information to patients who want it. That is the best audience.

Those who seek to exploit EHRs — and there are many non-health related data acquirers who are interested in this — will have no trouble cajoling, tricking, deceiving, cheating, misleading, and generally inducing patients into giving up their EHRs for non-health purposes. Requirements for consent or authorization will not work either. Records obtained by patients will have no procedural prerequisites before the records can be shared with third parties. If there is money to be made by obtaining records from the health care system with patient approval, those who seek to profit will find a way to comply with any access requirements. Remember too that it only takes one slip for a patient's entire health history to end up in the hands of a data broker. Once

---

[17] See generally World Privacy Forum, Many Failures – A Brief History of Privacy Self-Regulation (2011), https://www.worldprivacyforum.org/2011/10/report-many-failures-a-brief-history-of-privacy-self-regulation/.

[18] See World Privacy Forum, A Patient's Guide to HIPAA, https://www.worldprivacyforum.org/2019/03/hipaa/; see also our Health Category page for additional materials https://www.worldprivacyforum.org/category/health-privacy/.

that happens, the record and its information will be gone forever, scattered in the files and profiles of untold numbers of companies.

Again, we recognize the many parties that want to use this type of data responsibly. We have watched the data arena for a very long time, and have well-grounded reason to believe there will be some quite serious abuses unless there are procedural or other protections put in place. It is in this context that we want to mention briefly the ways we have documented that health care data is utilized outside of the HIPAA-covered entity ecosystem.

WPF has written extensively about our research into data brokers and their impact on people. See *The Scoring of America* for detailed research about data brokers.[19] This report contains a section on using a variety of marketplace data to score consumers in the health arena. We have also testified about sensitive health data and the ways that it tends to escape the protections of the HIPAA data ecosystem. The harms and problems we have already documented have not gotten better; they have worsened. The fact patterns indicate that if HHS goes through with its proposal to allows patients to simply deliver their EHRs into non-health hands without any notice, education, or intervention, that an ugly free-for-all will ensue, one that is focused on acquiring detailed patient data for purposes of monetization.

We have written extensively about data broker *lists* in the past. These lists still exist, and they are shocking for people who are unaware of them. We have found lists of sufferers of particular diseases like asthma, heart disease, and literally thousands of ailments. We have found lists of people on specific prescription medications - including medications that are especially sensitive. We have found lists of people inferred to have certain diseases or conditions. But today, those lists that used to be on paper, are now digitized. Those digitized records are seldom used alone. Most often now, datasets with identifiable patient information are hosted on one or more cloud services, and a menu of APIs for rich and rapid data access along with add-ons of analytics services can be utilized together as a service.

In short, the data broker model has evolved radically. It is now possible (and simple) for health datasets to be found, acquired, and modeled analytically with real-time inferences. This is a positive development for healthcare when used for health-related purposes and covered under either HIPAA or the Common Rule. Full patient health records belong in the HIPAA-covered ecosystem when they are identifiable. Fully identifiable patient health records should not be so readily clicked over to non-health third parties without some vetting and determination of purpose.

Utilizing and analyzing individuals' health data is a big business, and there is a lot of profit involved in acquiring accurate health data to feed this engine. A leading source of this data will

---

[19] Pam Dixon and Bob Gellman, The Scoring of America, World Privacy Forum. April 2014. http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf

in all likelihood be the patient EHR as shared with third parties, unless HHS ensures there are sufficient procedural and administrative controls in place.

C. Things that might help

We wish we could offer a simple, one-step solution to the dilemma we identify here. We do not believe that there is any single magic bullet here. We offer instead some ideas and some thoughts that have some potential to help when used in combination.

Commission a Study: The full consequences for patients of the availability of EHRs that the NPRMs propose will be enormous. We believe that health care costs for everyone will increase, that the practice of medicine will change for the worse, and that patient privacy will be devastated as lifetime patient records leak out into the world. We acknowledge here, as we said in the introduction, that there are benefits as well. Nevertheless, the negative consequences will be significant and, for patients who allow their EHRs to "escape" into the hands of data brokers, those consequences will last a lifetime and will affect their heirs. the Department should commission a study of all of the consequences before moving ahead. The National Committee on Vital and Health Statistics is one existing group that could be asked do a study without much effort or additional administrative steps. We would prefer to see the Department commission an advisory committee like the Secretary's Advisory Committee on Automated Personal Data Systems that first proposed FIPs in 1973.

Expand HIPAA: There are still health care providers and health plans not covered by HIPAA. This choice by the Department has already had many unfortunate consequences, and one is that EHRs covered by HIPAA end up in the hands of those not covered by HIPAA. A few of the problems raised by the NPRMs would be reduced or eliminated if the Department expanded HIPAA to cover all health care providers. The Department has the authority to accomplish this, and we think extending HIPAA to cover *all licensed health care providers* (regardless of their use of electronic transactions) would be most beneficial. This change will provide a measure of help. We admit it will not address the core of the privacy problem we identify, however, it still improves the overall picture.

Wait for Congress. The big problem and the principal cause of the dilemma in waiting for Congress is the absence of any general-purpose privacy law that covers the vast universe of data aggregators, collectors, analysts, and others waiting to get full patient records. We suggest that the Department ask for improved privacy protections for EHRs that end up in third party hands as a result of increased interoperability. We fully understand the frustrations of waiting for congressional action, and we urge HHS to create a safety net of procedural protections for patients. See next point.

Set Procedural Barriers. First, we do not propose limiting direct patient access, access by a patient's personal representative, a patient's lawyer, or another health care provider. However, we also recognize that unfettered access by third parties to patients' health records can create

systemic privacy problems. We already suggested modifying 45 CFR § 164.524(c)(3)(ii) to give covered entities a basis to resist transferring EHRs to most third parties outside the health care system. Other procedural barriers that focus on those who would exploit patient records for non-health purposes could help as well. When presented with a patient authorization from a data broker, marketer, or the equivalent, covered entities should be allowed to contact the patient, explain the type and potential consequences of the authorization, and give the patient the opportunity to change their mind. Also, regulations can make it easy for patients to limit an authorization that they have already signed, perhaps by the date of treatment, a restriction on what may be disclosed, require an additional authorization for genetic information, and a flat 30-day (or one-year) expiration date so that those seeking to exploit patient health records must obtain a new authorization. This will only help so much because the entire record will already have been obtained under the original authorization. But it could still be helpful. Allowing a 90-day waiting period could also be helpful. Used creatively, procedural barriers have potential to help.

Standards. We already said that industry self-regulation has no real hope of helping. We recognize that the authority of the Department to regulate third party users outside the health care system ranges somewhere between limited and non-existent. Nevertheless, inviting industry and consumers to work together to establish privacy standards and limits under the *OMB Circular A-119 - Voluntary Consensus Standards*, could prove beneficial. There are some better players in industry who might accept this approach. For the US definition of VCS, and the baseline procedures that must be in place, see *OMB Circular A-19* at: https://obamawhitehouse.archives.gov/omb/circulars_a119

We understand that the crooks, quacks, and charlatans waiting to exploit EHRs will ignore standards activities, but the Department may make some progress by appealing to the better nature of reasonable actors. There are so few options to ameliorate the situation that this has some appeal despite the inherent limitations. The Department's role can be limited to that of convener, with the real burden shifted to those willing to develop and accept the standards.

Specific steps to take in this NPRM. We recognize that there is only so much that the Department can do in this NPRM and in the context of the HIPAA privacy rule. However, there are steps that might help.

The improved NPP that the NRPM proposes could be adjusted to require that any place where an NPP mentions third party access, the notice must include a statement like this:

> **Any health record given to a third party outside the health care system will not be protected by the HIPAA health privacy rule in the hands of that third party. Your health information might be sold, shared, or otherwise utilized by that third party.**

A notice like this might make some patients think about before authorizing disclosure.

We wish it were possible to do more than just a notice, and we would certainly welcome other steps. What is most important is that the Department step up to the plate and take some action, any action, that will warn patients about the consequences of data sharing. To date, Departmental actions are solely facilitating use of patient data by any and all third parties without any steps to recognize the dilemma that we identify in these comments: not all third parties are trusted third parties.

We thank you for the opportunity to submit these comments.

Pam Dixon,
Executive Director
World Privacy Forum
www.worldprivacyforum.org