



# WORLD **PRIVACY** FORUM

**Comments of the World Privacy Forum  
Regarding  
Confidentiality of Substance Use Disorder (SUD) Patient Records, 42  
CFR Part 2, 45 CFR Part 164. RIN 0945-AA16**

*Sent via email and Regulations.gov*

US Department of Health and Human Services  
Office for Civil Rights  
Attention: SUD Patient Records  
Hubert H. Humphrey Building  
Room 509F  
200 Independence Avenue SW  
Washington, DC 20201

26 January 2023

The World Privacy Forum (WPF) welcomes the opportunity to submit comments on the Notice of Proposed Rulemaking to modify the requirements for substance use disorder (SUD) treatment records protected by Part 2 regulations (42 CFR Part 2).<sup>[1]</sup> The changes seek to implement section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.<sup>[2]</sup>

The WPF is a nonprofit, non-partisan 501(c)(3) public interest research group. WPF focuses on multiple aspects of privacy, with health privacy and health data governance 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. We testify before Congress and federal agencies, and we regularly submit comments on HIPAA and related regulations.<sup>[3]</sup> WPF participates in the World Health Organization, and serves as a co-chair of its Research, Academia, and Technical

constituency, as well as serving as a member of a 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>.

## **I. General Comments**

Protecting Substance Use Disorder (SUD) treatment records from unwanted uses and disclosures in order to assure the individuals who are seeking treatment that they will not face prosecution or other unwanted consequences is certainly a worthy goal. Providing these greater assurances is obviously the primary objective of the changes to Part 2 directed by the CARES Act.

Existing Part 2 rules can create complex problems for the health care system and for others. For example, because the protections afforded by current Part 2 rules “follow the records” that are disclosed in accordance with Part 2, any entity that receives these records and who is not already a Part 2 provider faces a new and significant challenge. In some contexts, Part 2 records can be profoundly challenging for providers and others because of governance complexities and the potential for increased risks that they bring to some recipients. The core of the problem is that existing Part 2 rules are both different and stricter than the privacy rules otherwise applicable to health or other records that recipients maintain under broader HIPAA regulations.

Anyone working under a different privacy regime – and we observe that the Part 2 rules predate the HIPAA environment by many years – faces a major challenge in complying with the Part 2 rules as well as the other applicable privacy rules. Frankly, we believe that it is likely that many recipients do not comply with the Part 2 rules or even know that they are obliged to comply.

Problems with the sharing of Part 2 records extend beyond the health care system. Some SUD patients are homeless or receive services from homeless service providers. Continuum of Care (CoC) programs in many places promote community-wide commitment to the goal of ending homelessness. Nonprofit providers and state and local governments often work jointly to help homeless individuals and families. Information sharing among community providers is a feature of many of these programs, and some groups involved in CoC activities are covered by Part 2. The challenge of information sharing by Part 2 programs arises in the homeless world just as in the health care world.

Congress wants HHS to address these problems by changing the Part 2 rules to recognize the HIPAA rules and the need of non-Part 2 organizations to process Part 2 records in more standard ways. There is something of a damned-if-you-do and damned-if-you-don't quality here. While we recognize that everyone involved here is trying to do the right thing, problems remain nonetheless. The more that Part 2 records are used and disclosed in a manner similar to other records, the more the records are vulnerable to unwanted uses and disclosures that undermine the ultimate objective of providing additional protections for SUD patients and encouraging them to seek treatment. This is

a consequence of integrating Part 2 activities more closely with other health care activities and systems. HHS is already fully aware of the issues we raise here. We do not have a broad solution to this dilemma, but we think it worthwhile to acknowledge it overtly.

## **II. HHS Should Cover All Part 2 Programs under HIPAA**

Coordinating rules for SUD records is challenging enough for Part 2 programs that are subject to HIPAA. It is a challenge as well for other health care entities that are only directly subject to HIPAA, but that occasionally receive Part 2 records. There is another class of entity, namely Part 2 programs that are not subject to HIPAA. This creates three classes of programs:

- HIPAA-covered entities;
- Part 2 programs subject to HIPAA;
- Part 2 programs not subject to HIPAA.

These three classes of programs add substantial layers of complexity to the existing rule and the proposed changes.

To solve some of the problems, we suggest that HHS require all Part 2 programs to comply with HIPAA rules. This will simplify the transfer of records as appropriate between HIPAA-regulated programs and Part 2 programs as well as transfers between the two types of Part 2 programs. It will also simplify the rules. Our suggestion here will not solve the basic dilemma that we noted in the last section of these comments, but it should make things somewhat easier for all.

Further, Part 2 programs not currently under HIPAA do not necessarily offer their patients the full range of protections that HIPAA privacy and security rules require. While Part 2 rules offer better protections for patients in some ways, many parts of HIPAA mandate better and more specific patient protections.

We note that while today, HIPAA rules apply broadly to health care treatment and payment activities, there are still gaps in the protections that patients (and health care providers!) often do not realize exist. These gaps create major threats to patient privacy and security. The gaps also create significant confusion. Health care activities not necessarily covered by HIPAA include:

- Free clinics;
- Cash-only providers; and
- The National Institutes of Health.

We would urge HHS to extend HIPAA to *all* health treatment activities without exception. We recognize that this is not the appropriate rulemaking for that recommendation. What is appropriate here with this rulemaking, however, is to take the opportunity to end one particular class of non-HIPAA healthcare programs that is present. That is why we ask

HHS to extend HIPAA requirements to all Part 2 programs. Every little bit helps. Less confusion will help SUD patients and better protect their records, and better fulfill the goals of the CARES Act.

### **III. Definition of *Intermediary***

Based on our limited knowledge of homeless activities, we wonder if the definition of *intermediary*, or the commentary about it, should acknowledge that limited information about Part 2 patients may, at times, be appropriate for sharing within a Continuum of Care. The focus of the definition seems to be on sharing within the health care world.

The assistance provided to homeless SUD patients may be just as important in some cases as health care coordination. We also wonder if there may be a role for homeless providers, a continuum of care, or similar homeless service organizations as a *qualified service organization*.

We admit to a significant degree of uncertainty here, and we suggest that HHS may need to ask HUD for assistance on this point. Seeking express consent for disclosures to homeless providers may be appropriate here, but there may be a need for flexibility among homeless providers whether they receive Part 2 data with or without consent.

### **IV. De-identification of Records**

We observe that the HIPAA de-identification standard discussed and referenced in several ways in the NPRM is old and very much out of date. The standard is in great need of updating and tightening. The Part 2 rulemaking is not the place for a change in that de-identification standard, but HHS should be looking at the problem otherwise.

### **V. Notice and Consent**

The patient notice requirement in the proposed rule places an even greater burden of reading and understanding a privacy notice on SUD patients than on HIPAA patients. Further, the proposed rule allows a patient to consent to a broad range of Treatment, Payment, and Operations (TPO) disclosures and for that consent to be good forever unless revoked in writing. At the same time, the proposed notice requirements recognizes that SUD patients may at times lack capacity to understand the notice. We presume that the same lack of capacity applies to understanding consents and to managing revocation of consents. We recognize, as we must, that this result is directed by the statute. This is not HHS's doing.

We believe that one of the good things about HIPAA is that it removed the need for consent for most disclosures that support health care activities.<sup>[4]</sup> We hope that after all this time, at least some HIPAA patients learned that requests for consent for disclosure are unusual and should be carefully reviewed and questioned. The extent to which this is the case is, of course, uncertain.

The CARES Act continues to use the much-outdated notice-and consent model for regulating disclosures of particularly sensitive information by patients whose capacity to agree may be limited. Further, consent for TPO disclosures will likely be sought aggressively by SUD programs that want to receive payment. In some ways, this is a perfect storm of inappropriate reliance on notice and consent. This is another example of a damned-if-you-do and damned-if-you-don't policy. We admit, however, that we don't have a solution given the current model of Part 2.

Separately, we do support the proposed requirement that consent be required for disclosures for fundraising. We request and urge that this consent be required to be unbundled from other consents, so that patients are not asked to agree to marketing disclosures on the same page that includes a fundraising or a medical consent.

We have an additional small comment on notice. Patient notices may sometimes include citations to statutes and regulations. For most individuals who are not lawyers or federal employees, a citation to a statute or regulation is not useful. For example, few people know how to find something identified as *42 CFR Part 2*. We gently suggest that any notice that references a statute or regulation include a link that will enable the reader to find the item being cited. This should be easiest to accomplish when a notice is in digital format.

As a possible alternative, HHS should maintain a webpage aimed at patients that include current links to all Part 2 laws, rules, and explanatory materials. HHS should then require all patient notices and consent forms to include a link directly to that page. We note that conducting a keyword search on "42 CFR Part 2" on the HHS website leads to more than 1,600 results from HHS — which would be a lot for many patients to work through.

## **VI. Right to Request Restrictions**

With respect to the discussion of the right to request restrictions, we direct attention to WPF's Patient's Guide to HIPAA. FAQ #52 asks: "Why is the right to request restrictions almost meaningless?" [5] Part of the answer is that the rule does not require a covered entity to agree to a restriction requested by a patient. More importantly, the covered entity does not have to agree even if the patient's request is reasonable.

If HHS does not require a covered entity to respond to a patient's request for restriction, even to state whether the request is granted or declined, the right to request restrictions is meaningfully diminished. In some cases, the right to request restrictions will be — for all intents and purposes — abrogated in cases where the request is never given any response.

## **VII. Right to Direct Disclosures**

An existing provision of HIPAA (and one that we objected to at the time it was proposed) gives patients the right to direct disclosures to a person designated by the patient. See 45 CFR § 164.524(c)(3)(ii).

We said in comments filed in 2021 in response to a HIPAA rulemaking (86 Federal Register 5446, January 21, 2021):

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.<sup>[6]</sup>

We reiterate here in the context of Part 2 the point that we made then. All patients, including SUD patients, can be easily manipulated and induced to sign authorizations.<sup>[7]</sup> This type of inducement is no longer a theoretical issue, and has been well-researched and documented across sectors, including the health sector often through the use of “dark patterns” or “dark commercial patterns.”<sup>[8]</sup> Part 2 programs, whether HIPAA-covered entities or not, should hew to a higher standard. At a minimum, Part 2 programs need to be able to ask a patient who signed an authorization whether they understood the scope of the authorization and the consequences of signing it. That is doubly true when Part 2 records are within the scope of an authorization. We are not concerned here about consents for TPO disclosures.

Given the sophistication and ease of health records sharing interfaces today, we worry that Part 2 records will leak via unclear patient authorizations into the files of data brokers, marketers, and scammers. One consequence of any leakage is that the protections against law enforcement access and use will be undermined. It would only take one well-publicized incident for all Part 2 programs to acquire the reputation of conveyers of SUD patient records to the police.

We want all HIPAA-covered entities to have more ability to question at least some authorizations signed by patients. As we said in the earlier comments, when “Junk Mail America, Inc.” contacts a hospital with signed authorizations from 5,000 patients, the hospital has no grounds to contest the demand for records. We do not want mailing list brokers to be able to sell verified lists of drug abuse patients obtained as a result of induced or “nudged” patient authorizations.

If HHS is unwilling to solve this problem for everyone, then HHS should give Part 2 programs the right to intervene when presented with inappropriate patient authorizations. We observe in passing that none of the limits that the Department proposes to add in § 2.32(a)(1) will address disclosures made pursuant to patient authorizations.

### **VIII. Scientific Research**

The rule urgently needs a clear and contextually appropriate definition for *scientific research*. The first line of the Belmont Report appropriately states: “Scientific research has produced substantial social benefits. It has also posed some troubling ethical questions.” While the historic context of the Belmont Report was dire, ethical questions regarding scientific research are just as important now. Today, a social network that does “research” in order to improve the display of advertising to health care providers or to people with certain conditions could call that research “scientific” because the ultimate goal could be, for example, to see if better advertising ultimately improves patient outcomes. We need to do better than allow a laissez-faire approach to defining scientific research; we want to see a definition in this rule that precludes that type of marketing activity (or other activities sitting at ethical boundaries) from being characterized as “scientific research.”

Here, we urge that HHS cite and utilize the relevant sections of the foundational work that has already been done in this area. We include the Belmont Report <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html>, particularly Section A, *Boundaries between practice and research*, and Section B, *Basic Ethical Principles*.

We quote in full an important section on the test of beneficence in relation to amount of risk. The rule needs to address this issue. From the Belmont Report, Part B., B(2.) Beneficence:

The obligations of beneficence affect both individual investigators and society at large, because they extend both to particular research projects and to the entire enterprise of research. In the case of particular projects, investigators and members of their institutions are obliged to give forethought to the maximization of benefits and the reduction of risk that might occur from the research investigation. In the case of scientific research in general, members of the larger society are obliged to recognize the longer term benefits and risks that may result from the improvement of knowledge and from the development of novel medical, psychotherapeutic, and social procedures.

The principle of beneficence often occupies a well-defined justifying role in many areas of research involving human subjects. An example is found in research involving children. Effective ways of treating childhood diseases and fostering healthy development are benefits that serve to justify research involving children -- even when individual research subjects are not direct

beneficiaries. Research also makes it possible to avoid the harm that may result from the application of previously accepted routine practices that on closer investigation turn out to be dangerous. But the role of the principle of beneficence is not always so unambiguous. A difficult ethical problem remains, for example, about research that presents more than minimal risk without immediate prospect of direct benefit to the children involved. Some have argued that such research is inadmissible, while others have pointed out that this limit would rule out much research promising great benefit to children in the future. Here again, as with all hard cases, the different claims covered by the principle of beneficence may come into conflict and force difficult choices.

We also include the relevant definitions of scientific research found in the Common Rule, and we include the generally agreed upon definitions found in the International Compilation of Human Research Standards, 2020 Edition. <https://www.hhs.gov/ohrp/sites/default/files/2020-international-compilation-of-human-research-standards.pdf> . HHS needs to adopt a strong definition of “scientific research” which sits comfortably in the existing legal canon. For example, the National Science Foundation states:

The goals of the Common Rule apply to any person who has the potential to be harmed because of a research project, whether or not the person is directly interviewed or identified through data collected by another researcher for a different purpose. Public use data files are normally stripped of identifiable private information or "de-identified. In this case, the research is exempt since no identifiable human subjects are involved. (§ 690.102.f.2) When identifiers are included in the data, several issues should be considered:

The research project should be assessed for the likelihood that identified respondents could be harmed or easily identified. If the project is low risk then no special oversight is required. If the data is de-identified, then no "human subjects" are involved in the research. The project information should be kept confidential; the level of confidentiality commensurate with the level of risk applicable to all identified persons.

The regulations do not mandate informed consent from identified persons in secondary data sets although it may be required. If the potential risk is serious and not ameliorated by confidentiality procedures, then consent is necessary. Medical records may be subject to additional regulations.[9]

We can appreciate the challenges of ensuring a strong definition of scientific research. To leave this definition to the whims of interpretation is not a good choice for patients or HHS.

Thank you for the opportunity to submit these comments. We want to emphasize again the importance of HHS extending HIPAA requirements to all Part 2 programs, and to ensuring there is a strong definition of “scientific research” within the rule itself.



WPF is pleased to answer any questions and discuss these issues further.

Respectfully submitted,

Pam Dixon  
Executive Director,  
World Privacy Forum

## Notes

[1] <https://www.federalregister.gov/d/2022-25784>.

[2] Public Law 116–136, 134 Stat. 281 (March 27, 2020).

[3] 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/>.

[4] Some allowable disclosures are, in our view, inappropriate and overly unbounded (e.g., national security disclosures), but we are not addressing the scope of HIPAA disclosures in these comments.

[5] See World Privacy Forum, *A Patient’s Guide to HIPAA*, <https://www.worldprivacyforum.org/2019/03/hipaa/#c90>.

[6] <https://www.worldprivacyforum.org/2021/05/wpf-comments-on-hhs-proposal-to-change-hipaa/>.

[7] We note here the now well-understood field of research called “dark patterns,” which concerns itself with how people are nudged into consenting and making choices. See Federal Trade Commission Staff Report, *Bringing Dark Patterns to Light*, 22 September 2022. <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers>.

[8] Dark patterns in patient health: a 2022 European Commission study found that “nagging” was common in health websites and apps. *EC (2022) Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative*

*personalization. Final Report. Pages 53, 114.* <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1>

[9] *FAQ and Vignettes, Interpreting the Common Rule for the Protection of Human Subjects for Behavioral and Social Science Research*, National Science Foundation. <https://www.nsf.gov/bfa/dias/policy/hsfaqs.jsp#minimal>.