3108 Fifth Avenue
Suite B
San Diego, CA 92103

Comments of the World Privacy Forum
To
US Department of Health and Human Services Substance Abuse & Mental Health Services Administration regarding Confidentiality of Alcohol and Drug Abuse Patient Records Regulations, 81 Federal Register 6988 (February 9, 2016), RIN 0930-AA21, SAMHSA 4162-20

Via Federal eRulemaking Portal www.regulations.gov

Substance Abuse and Mental Health Services Administration,
Department of Health and Human Services,
Attn: SAMHSA-4162-20,
5600 Fishers Lane,
Room 13N02B
Rockville, MD, 20857

March 24, 2016

The World Privacy Forum welcomes this opportunity to submit comments on the proposed rule from the Substance Abuse and Mental Health Services Administration (SAMHSA), changing the Confidentiality of Alcohol and Drug Abuse Patient Records regulations, 42 C.F.R. Part 2. The proposed rule appears at 81 Federal Register 6988 (February 9, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-02-09/pdf/2016-01841.pdf. RIN 0930-AA21, SAMSHA 4162-20.

The World Privacy Forum is a non-profit public interest research and consumer education group. We publish research papers, policy comments, educational materials, news, and other materials focused on privacy and security issues. Much of our work explores technology and health-related privacy issues, biometrics, consent, data analytics, and many other rapidly evolving areas of privacy. Our publications and more information about our activities are at www.worldprivacyforum.org.

I. Introduction to World Privacy Forum Comments

In general, the World Privacy Forum supports SAMHSA's approach to amending the Confidentiality of Alcohol and Drug Abuse Patient Records regulations. The need for a separate and strict confidentiality regime for patients of Part 2 programs remains just as important today as in the past. The privacy rule issued by the Department of HHS under the Health Insurance Portability and Accountability Act (HIPAA) is not sufficient to meet the needs of Part 2 patients.

While we welcomed the HIPAA privacy rule, we believe that it allows for far too many nonconsensual disclosures from the records of patients who have average needs for confidentiality. Part 2 programs could not successfully operate – and patients would not seek needed treatments –without a stricter confidentiality regime than found in current HIPAA rules.

At the same time, we recognize that some adjustments in the Part 2 rules are necessary to reflect ongoing changes in the health care system and health care information technology. Although we broadly support the changes, we do have a number of specific concerns about the proposed rules.

Here is a brief summary of the most important aspects of our comments regarding the SAMSHA proposal:

- We found several definitional problems in the proposal. Problematic definitions include the definition of a *program, "holds itself out*," the proposed definition of a *record*, and the proposed definition of *patient identifying information*. These definitions are deficient for various reasons which we have discussed below, and we have suggested solutions and changes.

- We support the proposed changes to the scope of activities permitted by a QSO.

- We have major objections to the proposal to add to a consent form a "statement that the patient … confirms their understanding of the terms of their consent." The "understanding" proposal may be the single most anti-patient provision in the entire rule. We strongly recommend deleting the proposed requirement from the consent form. It serves those requesting consent, not the patients.

We discuss additional issues, including disclosures, research, internal confidentiality agreements, and data use agreements. Please see our detailed comments below.

II. Definition of program re: "Holds itself out" is too vague

The rule's definition of a *program* states that a provider that is not a general medical facility or general medical practice is a part 2 program if it is an individual or entity who *holds itself out* as providing, and provides substance use disorder diagnosis, treatment, or referral for treatment. We are troubled by the phase *holds itself out*. We recognize that the proposed rule tries to provide clarity with a new explanation:

> "Holds itself out" means any activity that would lead one to reasonably conclude that the individual or entity provides substance use disorder diagnosis, treatment, or referral for treatment including but not limited to:
> • Authorization by the state or federal government (e.g. licensed, certified, registered) to provide, and provides, such services,
> • Advertisements, notices, or statements relative to such services, or
> • Consultation activities relative to such services.

The problem here is that "hold itself out" is simply too vague to be clear in all circumstances. The phrase also focuses on the wrong element. What is most important is what actual substance abuse treatment services are being *provided*, not how a program *presents itself* to patients, to other providers, or to others who supporting substance abuse patients in other ways.

A patient who walks in the door of a health care facility may have no idea what services the facility "holds itself out" as providing. In all cases, it should be crystal clear to patients of these programs what confidentiality rules apply, preferably through overt labeling. How a program presents itself to various audiences should not be the determining factor.

We urge the adoption of a clearer definition and an overt labeling requirement in place of the vague standard.

In addition, we find the last phrase (consultation activities relative to such services) particularly unclear. Is a physical security company that provides consulting to services Part 2 programs a Part 2 program itself?

III. Definitional problems

We found several significant weaknesses in some of the proposed definitions.

A. Proposed definition of record does not address identifiability

The proposed definition of *record* is:

> Records means any information, whether recorded or not, received or acquired by a part 2 program relating to a patient. For the purpose of these regulations, records include both paper and electronic records.

The comprehensive nature of this definition is appropriate. However, the definition fails to address the issue of identifiability. We see the proposed definitions of *patient* and *patient identifying information*. However, the definition of *record* does not address identifiability.

Information that is not individually identifiable, that is not reasonably capable of being reidentified, or that is aggregate may not need to be covered by the definition of record. The statement "we saw ten patients today" is a *record* under the definition, but it does not need the protections afforded to identifiable records. We also suggest that the definition might include *created by* in addition to *received or acquired*.

B. Proposed definition of *patient identifying information* is substantially insufficient to protect patients

The proposed definition of *patient identifying information* is:

> Patient identifying information means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient, as defined in this section, can be determined with reasonable accuracy **either directly or by reference to other publicly available information**. The term does not include a number assigned to a patient by a part 2 program, if that number does not consist of, or contain numbers (such as a social security or driver's license number) which could be used to identify a patient with reasonable accuracy from sources external to the part 2 program.

We call specific attention to the words in bold.

First, we are not sure of the purpose of the word *other* in *other publicly available information*. What publicly available information is referenced here? An SSN or a fingerprint is not publicly available information.

Second, we do not understand why only publicly available information is relevant to identifiability determinations. A patient identified through use of non-publicly identifiable information (e.g., an employer record, a police file, or another health record) is just as harmed as a patient identified through wholly public records. We urge deleting the words above in bold entirely.

Third, the definition should mention *other identifiers assigned to an individual, including but not limited to credit card numbers, driver's license numbers, automobile license numbers, telephone numbers and IP addresses*.

Finally, we think the definition fails to recognize that individuals can be identified through non-unique identifiers. It has been widely reported and documented through now unambiguous research that most Americans can be uniquely identified from their gender, five-digit zip code, and date of birth. We suggest you consider using this phrase from HIPAA definition of *individually identifiable health information*: "[information] with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."

These changes would go far to improving and strengthening the definitional issues in the proposal.

IV. Qualified Service Organization

We do not object generally to the changes proposed for the scope of activities permitted by a QSO. We note these comments by SAMHSA:

> Accordingly, SAMHSA has consistently articulated in applicable guidance that a QSO would be permitted to disclose the part 2 information to a contract agent if it

> needs to do so in order to provide the services described in the QSOA, and as long as the agent only discloses the information back to the QSO or the part 2 program from which the information originated. If a disclosure is made by the QSO to an agent acting on its behalf to perform the service, both the QSO and the agent are bound by the part 2 regulations, and neither organization can disclose the information except as permitted by part 2 and SAMHSA's interpretive guidance.

We think that these restrictions are entirely appropriate and need greater emphasis and, perhaps, enforcement. We have seen hints that some Part 2 programs may casually use the QSO structure in some circumstances as a general way to evade Part 2's strict limits on use and disclosure.

V. Problematic Patient Consent Issues: WPF strongly urges changes

We note and support (§ 2.31) the proposed inclusion of a general designation in the "To Whom" section of the consent form. The proposal seems to us to strike a reasonable balance among the interests involved here, while protecting confidentiality. We leave it to others to address in more detail any operational consequences, but we believe that protecting confidentiality must remain the highest value here.

However, we have major objections to the proposal to add to a consent form a "statement that the patient … confirms their understanding of the terms of their consent." Someone signing a complicated consent form may or may not actually understand the form or the consequences of what they are agreeing to. A statement that says "I understand the terms" may not be read, and it may not be true.

How many times have the readers of this comment checked a box on a webpage or phone app that says "I have read the terms of service" when they have in fact not read the terms? It is standard practice of most people to check boxes or agree to statements whether they are true or not. This is especially true in electronic devices, where people are especially inclined to tick a box or push a seemingly simple "I agree" or "Next" button. Knowing what people do, an unscrupulous company makes customers "agree" to things that the company knows are not true in the hope of improving the company's legal position if and when litigation ensues. The "agreement" rarely has the desired effect, but companies do it anyway.

A signed statement about reading or understanding says nothing about the actions or understanding of the signer. The only way to determine understanding is to ask specific questions that reflect true understanding, and that is not a realistic possibility. A statement about understanding only serves the interest of those collecting the consent, and the statement will only be used against the signer.

It would be in any signer's interest to cross out the proposed statement. Would SAMHSA consider a consent form valid if a patient crossed out the statement about understanding? Would an average patient's understanding be the same as the average lawyer's understanding? If a patient does not fully understand the consent form, is that patient therefore incapable of giving consent?

We think that SAMHSA would be better off not delving into the realm of actual understanding. Leave it to be determined if and when it arises. The "understanding" proposal may be the single most anti-patient provision in the entire rule. We strongly recommend deleting the requirement from the consent form.

VI. List of Disclosures

The proposal adds (§ 2.13(d)) a requirement that patients must be provided with a list of entities to which their information has been disclosed pursuant to a general designation in a consent form. The World Privacy Forum supports making a disclosure history available to patients in all circumstances. We observe that this requirement will overlap with the HIPAA requirement for which OCR has yet to finalize the rule.

We suggest that the rule in § 2.13 should be broadened in several ways.

First, many modern health care information systems routinely record all uses and disclosures. When a record of uses and disclosures already exists, a program should be required to make that record available to a patient upon request. It may actually be easier and less expensive to share a complete list of uses and disclosures rather than a more selective list. We propose this for programs that otherwise maintain a record of uses and disclosures. If a program does not maintain that record, then we support applying the proposed requirement to that program. Of course, while we prefer to provide a list of both uses and disclosures that are available, we support as a second choice just providing a list of all available disclosures. The proposed rule is narrower and is a third choice.

Second, the proposal limits providing a list of disclosures to those made within the last two years. We suggest that programs be required to provide a list of disclosures for at least the last two years and that the requirement include any earlier disclosures requested by a patient if the program can readily retrieve them.

In many cases, it is as easy to retrieve a list covering ten years as it is to retrieve a list covering two years. If the capability exists and the list can be retrieved without significant additional cost, then the patient should be able to have an expanded list of disclosures. If the patient wants the list and the list is readily retrievable, there is no reason not to fulfill the request. Note that we are not proposing that the rule require retention of a list of disclosures for a period greater than two years, but any program that maintains a disclosure history is highly likely to keep that history for a very long time.

The burden of making older disclosure information available will be small. We note in passing our agreement with SAMHSA's observation: "SAMHSA anticipates that there will be few requests based on the relatively small number of accounting requests that most covered entities have received to date under the HIPAA Accounting for Disclosures rule, according to some anecdotal reports." We observe that the few patients that want older disclosure records will likely be able to obtain the records through a lawsuit, and if only one lawsuit is avoided, a more generous rule will be worth it.

VII. Research Provisions

We have a problem with several aspects of the research provision. We do not object to research uses of Part 2 information under appropriate circumstances. At a minimum, all research using Part 2 patient information should be required to obtain a certificate of confidentiality. We admit to having some uncertainty about the value of a certificate, but there is no doubt that both patients and researchers are better off if a certificate applies to a research project. We think that the regulation should mandate a certificate of confidentiality as a prerequisite to researcher access to Part 2 information.

In that vein, we applaud this requirement in § 2.52:

> (b) Any individual or entity conducting scientific research using patient identifying information obtained under paragraph (a) of this section:
> (1) Is fully bound by these regulations and, if necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by these regulations.

We think the words could be clearer. The phrase "will resist in judicial proceedings" is a bit ambiguous. It implies resistance *to* judicial proceedings, which may not be the intended meaning. We suggest this alternative: "will resist any administrative, judicial, or other request or demand for access to patient records (except as permitted by these regulations), if necessary, by challenging the request or demand in a proceeding before a court of competent jurisdiction."

We have another suggestion. We recognize that the proposed provision in § 2.52(b) imposes limitations on qualified researchers who obtain Part 2 records. We would be much happier if the rule required researchers to sign an acknowledgement or (better yet) a data use agreement that expressly acknowledged the specific limitations. SAMHSA could prepare the requisite documents for everyone to use.

It is one thing for a regulation posted somewhere on the Internet to limit a researcher's conduct, and it another thing altogether for a researcher to be obliged to sign a formal statement to that effect. Statements that must be signed tend to be read and to be reviewed by lawyers, who may actually be useful in this context, by telling researcher expressly what they can and cannot do.

VIII. Other Ideas

SAMHSA asked for input on several other topics , and we provide a response to some of those requests here.

A. Data Use Agreements

We strongly support the use of data use agreements for all research transfers of Part 2 information. We made this point just above in our comments on research. Data use agreements specifically inform researchers, their institutions, lawyers, privacy officers, and security officials what obligations come with the data. A data use agreement can be as long as needed, and it can cover matters not appropriate to include in regulations. We suggest that SAMHSA prepare and

circulate one or more sample data use agreements so that everyone is not obliged to reinvent the wheel each time.

B. Use of internal confidentiality agreements

We also support the use of internal confidentiality agreements for staff members who have access to patient identifying information and other confidential data. Breaches and misuse of information can result when users of data are not fully aware of the data's sensitivity and of the consequences of violating the rules. No user of data should ever be able to say, "I didn't know that the data was sensitive" or "I didn't know that I wasn't allowed to put the data on my laptop/tablet/phone."

There is no substitute to telling individuals repeatedly about their obligations and the consequences for all of not complying. The signing of confidentiality agreements should be an annual ritual. We have seen reports of uninformed staff sharing records with police in violation of the rule, presumably for lack of understanding of the program's obligations. The obligation to sign an internal confidentiality agreement may help correct lapses in this important area.

IX. Conclusion

Thank you for the opportunity to submit these comments. We are pleased to discuss these comments and any questions you may have. Please do not hesitate to contact me.

Respectfully submitted,

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