WORLD PRIVACY FORUM

3 Monroe Parkway
Suite P #148
Lake Oswego, OR 97035

Comments of the World Privacy Forum

Regarding

**The Department of Health and Human Services, Office for Civil Rights,
Request For Information RIN 0945–AA00, Docket ID HHS–OCR–0945–AA00**

Via http://www.regulations.gov

U.S. Department of Health and Human Services
Office for Civil Rights
ATTN: RFI, RIN 0945-AA00
Hubert H. Humphrey Building
Room 509F
200 Independence Ave SW
Washington, DC 20201

January 24, 2019

RE: Department of Health and Human Services, Office for Civil Rights RIN 0945–AA00 regarding possible changes to the HIPAA health privacy and security rules

We welcome the opportunity to respond to the Department of Health and Human Service's (HHS) Request for Information regarding possible changes in the HIPAA health privacy and security rules. The Federal Register notice appeared on December 14, 2018, 83 Federal Register 64302, https://www.federalregister.gov/documents/2018/12/14/2018-27162/request-for-information-on-modifying-hipaa-rules-to-improve-coordinated-care.

The World Privacy Forum is a nonprofit, non-partisan 501(c)(3) public interest research group. The WPF focuses on privacy, with health privacy being among our key areas of work. We have published a large body of health privacy work, from guides to HIPAA to reports and FAQs for victims of medical identity theft, to genetic privacy, precision medicine, electronic health records, and much more. We have testified before Congress and federal agencies, and have submitted extensive previous comments on HIPAA and related regulations. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and public comments at http://www.worldprivacyforum.org.

Introduction

HHS published a relatively short document describing the issues on which it seeks comment. Although the RFI document itself is fairly brief, the RFI raises a large number of quite complex matters regarding potential changes to HIPAA, including how privacy works under the HIPAA privacy rule. For these comments we have selected those issues which impact privacy interests meaningfully.

The RFI states:

> OCR seeks public input on ways to modify the HIPAA Rules to remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and to promote the transformation to value-based health care, while preserving the privacy and security of PHI. Specifically, OCR seeks information on the provisions of the HIPAA Rules that may present obstacles to, or place unnecessary burdens on, the ability of covered entities and business associates to conduct care coordination and/or case management, or that may inhibit the transformation of the health care system to a value-based health care system.

In addition to being complex, some of the proposals in the RFI impact privacy interests quite substantially. However, of all of the issues raised in the RFI, we are most concerned about the prospect of compelled, mandatory disclosures of patient information, which we discuss in section III of these comments, which responds to A. 7 of the RFI.

Compelling disclosure for treatment will open the door to conflicts that cannot be resolved by other means. There will no longer be any middle ground available. One provider will simply demand production of a patient record, and the other provider will have no choice. There needs to be some give in the system to cover hard cases, and the current rule is adequate for that purpose. This is an area of very significant concern for us regarding the RFI.

Following are our detailed comments on the proposals in the RFI that meaningfully impact privacy interests and concerns.

Index to Comments:

Comments

I. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 2: Patient access to records

RFI Question A. (2):

How feasible is it for covered entities to provide PHI when requested by the individual pursuant to the right of access more rapidly than currently required under the rules? (The Privacy Rule requires covered entities to respond to a request in no more than 30 days, with a possible one-time extension of an additional 30 days.). What is the most appropriate general timeframe for

responses? Should any specific purposes or types of access requests by patients be required to have shorter response times?

We recognize the issue that HHS raises in this series of questions about the timeliness of patient access to records. Based on anecdotal evidence that has come our way, we think that patients too often have a problem getting timely access to records. However, we also recognize that revising the rule to make distinctions between classes of records will most likely not help patients all that much and will further complicate the request process. Those covered entities that miss deadlines today will simply miss new deadlines. Adding new entities (clearinghouses) to the mix of those with responsibility will only add to the overall confusion and allow entities to shift responsibility to others.

We would not oppose with any strength a proposal to shorten the time for covered entity response to a patient records for access to or a copy of a record. We might prefer a rule that required covered entities to make best efforts to provide prompt access to patients and for HHS to enforce that standard through audits and compliance reviews. Large institutions could do more to educate patients on record access by describing categories of records, explaining the time it takes to find them, and giving patients more granular choices. If patients knew how, they might ask for records about a particular visit or covering a specified time period rather than a copy of "every" record. The result might serve both covered entities and patients better.

We offer a different idea for consideration in addition to other proposals. Suppose HHS required covered entities to post on their websites the average response time (along with other statistics) about patient requests for access or a copy of a record. We would request that large institutions update their statistics once a month, smaller institutions four times a year, and small offices once a year.

This would help in several ways. Patients would know what they can expect from any given institution. Local reporters would be able to write about this aspect of HIPAA compliance, and that would encourage covered entities to do better. State legislators would be able to see the degree of compliance with covered entities in their states, and they could pressure the entities to do better though oversight and, if necessary, legislation. Publicity would allow covered entities to tout their prowess in responding as a way of attracting patients. The information would also be useful to OCR or other health privacy overseers so that those covered entities doing a bad job in responding would receive more attention and compliance audits.

We do not always favor what might be called a "market-based" response to problems, but we are not convinced that patients will understand or benefit from a more complex process. While the circumstances are not similar, we observe that the federal Freedom of Information Act imposes deadlines on agencies to respond to requests promptly. Despite all the attempts by Congress to adjust the mandatory response period and to encourage compliance, agencies often fail to meet deadlines, sometimes by years. There are limits to what can be accomplished through mandates.

At the same time, we think that HHS should find a way to encourage covered entities to do a better job of providing patients with direct access to their records and with the capability of

downloading copies of records. The spread of electronic health records should simplify patient access, and better health record technology may make some of the access problems go away.

One action that might help generally is if HHS removed some or all of the exceptions to patient access in the current rule. Other state and federal laws that provide for unrestricted patient access to records have not, to our knowledge, presented any sizeable problems. If covered entities did not have to review records to determine which portions could be withheld, the process of patient access would be simpler and faster.

II. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 5

> RFI Question A. (5):
>
> (5) Health care clearinghouses typically receive PHI in their role as business associates of other covered entities, and may provide an individual access to that PHI only insofar as required or permitted by their business associate agreement with the other covered entity, just as other covered entities, when performing business associate functions, may also provide access to PHI only as required or permitted by the business associate agreement(s) with the covered entity(ies) for whom they perform business associate functions. Nevertheless, the PHI that clearinghouses possess could provide useful information to individuals. For example, clearinghouses may maintain PHI from a variety of health care providers, which may help individuals obtain their full treatment histories without having to separately request PHI from each health care provider

While we like the goal of making patient access to their records easier, we do not see clearinghouses as helpful in achieving that goal. We have never met a consumer who has heard of or understood the role of a health care clearinghouse. In our *Patient's Guide to HIPAA*, we mention clearinghouses only when explaining their status as covered entities and never again thereafter. https://www.worldprivacyforum.org/2013/09/hipaaguide9-2/ (FAQ 9 in the Patient's Guide). We found no reason to ask consumers to understand the inner workings of the health care system.

If patients seeking their own records must contend with another obscure (to them) entity and then must confront the issues as known health care providers pass the buck to clearinghouses (and vice versa), the result will be more confusion. Further, institution will blame either other for failure to comply with the rule, and patients will not know who is responsible for the inevitable problems.

In general, the problems that the RFI identifies with respect to clearinghouses derives in significant part from the original decision to treat clearinghouse as covered entities rather than as business associates. Clearinghouses hold health information, but they do not function with respect to patients in the same way that the other covered entities (providers and plans) do. They

have authority as covered entities to make disclosures (e.g., for national security, law enforcement, and other purposes) that they do not need and that are inappropriate for them to make. That is one reason they end up subject to limits from business associate contracts. Covered entities do not want clearinghouses to make disclosures that the entities themselves should control. If patients understood what clearinghouses do, they would not want the clearinghouses to have broad authority to share patient records to remote purposes.

It would be better if HHS revised the rule to provide explicitly that clearinghouses are not covered entities. Clearinghouses should operate only under contracts with the covered entities that they serve. This is especially appropriate given that recent rule changes applied the HIPAA rules directly to business associates. HHS could provide – or encourage the industry to provide – standard contacts covering the business associate arrangement with covered entities. Clearinghouses should play a role in providing patient access only as directed by their customers, the providers and plans that they work for.

III. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 7, requiring mandatory disclosures for treatment and extending required mandatory patient disclosures to health care operations

> RFI Question A. (7):
>
> (7) Should covered entities be required to disclose PHI when requested by another covered entity for treatment purposes? Should the requirement extend to disclosures made for payment and/or health care operations purposes generally, or, alternatively, only for specific payment or health care operations purposes?

The answer to the first question about requiring disclosures for treatment is **No.** The answer to the second question about extending required disclosures to health care operations is ***Hell No***.

We support the existing rule's choice to allow disclosures for the treatment of any patient. That choice balances the interests of all involved in a fair way. Any patient has an equal chance of benefiting from a disclosure to a provider from another patient's record, and better health care for all is a fine goal. But the disclosures are, as are nearly all other disclosures, discretionary. There are times and circumstances in which a health care provider can and should refuse a disclosure. For example, suppose the patient whose record is sought for treatment is the record of the President of the United States. A physician treating another patient cannot be given the ability to compel the disclosure of the President's record because that physician thinks it might be useful in treatment of John Doe.

Instead of the President, consider compelled disclosures from the records of other elected officials, celebrities, and other public figures. Those who make their disease a matter of public record by promoting education or raising money would be most at risk, as patients might demand the same treatment that a particular public figure received. Similarly, a compelled disclosure of one patient's especially sensitive record involving sexual history or mental health may be

entirely inappropriate notwithstanding the possibility of value to another patient. Similarly, compelled disclosures of patients who are working undercover in law enforcement capacities would be at very significant risk, as would victims of domestic violence and other crimes.

A provider today can say to a patient, with a straight face for the most part, that the provider will not disclose that patient's record without legal compulsion. But no reassurance to a patient that the patient's record will be held to the high possible level of confidentiality will be available if any treating physician anywhere in the country (or in the world) could demand disclosure for treatment of another patient.

We observe that even the existing rule allows for a middle ground. It allows treating physicians to consult with each other without any exchange of identifying information about any patient. There is no need to go beyond the existing compromise.

We are deeply concerned about the prospect of compelled, mandatory disclosures. Compelling disclosure for treatment will open the door to conflicts that cannot be resolved by other means. There will be no middle ground available. One provider will simply demand production of a patient record, and the other provider will have no choice. There needs to be some give in the system to cover hard cases, and the current rule is adequate for that purpose.

We want to further discuss the predicament for victims of crime and domestic violence. This vulnerable population often fears getting health care because their abuser is someone who has legitimate access to health care records. This can include physicians, nurses, physician's assistants, people with access to billing, various business associates, and so on. If the rule is expanded to compel disclosure, we predict that victims of crime and domestic violence would experience even more difficulties than they do today, difficulties which can impact safety and even be life-threatening in certain circumstances. These circumstances occur too frequently to be ignored. Beyond the safety issues, we bring forward the additional issue of the need to harmonize any changes to the HIPAA privacy rule with the Violence Against Women Act, which has considerable privacy protections for victims of crime.

The only exception to consider is that if the disclosure of a patient's records is for the treatment of that same patient, then compulsion may be appropriate with the written consent of the patient. There is no need to balance interests when only one patient is involved, and especially when that patient consents to the disclosure. We are aware that problems do arise when one institution refuses to share a patient's record with a provider from another institution who is treating the same patient. However, no matter what the rule says, an institution that wants to impose a barrier will always find a way to do so. It appears that at least some of the existing problems result from lack of knowledge of the rules and lack of training.

We distinguish on the same grounds disclosures for payment. If the disclosure by one provider to another relates to payment for the same patient, the disclosure is appropriate. Otherwise, the balance of interests that we see as allowing treatment disclosures for another patient is tilted. Compulsion would allow one hospital to demand of another all the billing records from the treatment of all patients with a particular condition so that the hospital seeking the records could learn if there are approaches that would allow for increased billing opportunities. We see no

reason for compelling disclosures about payment, and we observe that the same problems with records about public figures will arise.

Finally, with respect to health care operations, we observe that the definition of *health care operations* in the rule is a 400-word monstrosity. It allows for countless different types of disclosures, some appropriate, some questionable, and some that should not be allowed. We have heard about actual or possible abuse of the health care operations definition by institutions that interpret the rule to allow them to do as a health care operation something that they could not do as a research or other type of disclosure. We suggest that it would be useful for HHS to collect facts on the abuse of the health care operations provision before making any changes that would allow for more data sharing. Some health care institutions and their lawyers think that *health care operations* means anything they want to do with records is permitted because of the vagueness of the term.

Extending the possibility for abuse by allowing one covered entity to demand the disclosure of broad classes of patient records on the grounds that the requester wants to engage in some vaguely defined health care operation would compound the felony. Imagine a requesting institution that wants many patient records to engage in a health care operation that the requester considered to be inappropriate or illegal. The result could easily be litigation that would be expensive and embarrassing to all, including HHS if it allowed a change in the role that gave requesters rights to demand disclosure and data holders no grounds on which to refuse.

We further note that if a hacker has gained unauthorized access to a health care operations system, it could well be a hacker making the request for mandatory disclosure of broad classes of patient data. HHS's data breach roster contains many examples of serious hacker intrusions. These would have more profound consequences if they could then demand patient data from other covered entities under the guise of stolen credentials.

WPF researched and published the first public report about medical identity theft in 2006, and we have continued publishing and researching and working in this area. (See: https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/. See also WPF's Medical Identity Theft Page, https://www.worldprivacyforum.org/category/med-id-theft/) We have robustly documented that medical identity theft operators are sophisticated and organized, and if a broad request via health care operations could be accomplished, it would be seriously abused by cybercriminals. The health care sector would be left with a serious mess on its hands.

Unless there is more evidence of a problem for treatment or payment disclosures with respect to the same patient, we strongly urge HHS to leave this part of the rule alone. If there are documented problems with disclosures for care coordination, then find a narrow solution that relates to the appropriate sharing of information about the same patient. If there are disputes or disagreements between institutions, then ask the patient to decide if a record should be shared.

Writing a rule that takes the patient out of the equation is inappropriate and wrong. Do not take away the patient's role in consenting to uncertain or questionable disclosures by substituting a policy that makes disclosure mandatory regardless of patient wishes. There is too much of that in

the existing rule already. If anything, the provision regarding health care operations should be narrowed and clarified to prevent abuse.

Expanding compelled disclosures of identifiable patient information could well result to a revolt by patients angry over more sharing of their records with no visible benefit to themselves. We might be happy to lead that revolt.

IV. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 9, adding requirement for disclosure of Protected Health Information to non-covered health care providers

> RFI Question A. (9):
>
> (9) Currently, HIPAA covered entities are permitted, but not required, to disclose PHI to a health care provider who is not covered by HIPAA (i.e., a health care provider that does not engage in electronic billing or other covered electronic transactions) for treatment and payment purposes of either the covered entity or the non- covered health care provider. Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to any of the matters discussed in Questions 7 and 8? Would such a requirement create any unintended adverse consequences? For example, would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester? Do the risks associated with disclosing PHI to health care providers not subject to HIPAA's privacy and security protections outweigh the benefit of sharing PHI among all of an individual's health care providers?

We suggest a completely different solution here. The rule should be extended to cover all health care providers, regardless of their use of electronic transactions. The public has no understanding of the limit of the rule in this respect. Individuals assume that the HIPAA rule covers all health providers without limit. If the rule applied to all providers, then the basis for this question disappears. HHS has authority to extend the rule to all health care providers. One approach is to declare that once a health care provider works in a HIPAA-covered environment, that provider remains subject to HIPAA no matter where that provider practices within the United States.

Any attempt to draw distinctions in use and disclosure policies between providers who are covered entities and those who are not covered entities will only create confusion and delay. Every legitimate request for disclosure will require a review of credentials and purposes in order to determine whether the disclosure is to a covered or non-covered entity. We also remind HHS that the rule allows for numerous disclosures to the police, intelligence agencies, public health agencies, and many more institutions that are not covered by HIPAA. We are more concerned about how these institutions, many not covered by any privacy law at all, treat health records that they receive under HIPAA. Addressing that major loophole in HIPAA seems to us to be higher priority than worrying about the use of patient records by health providers not subject to HIPAA but who are still subject to state laws and ethical standards.

V. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 11

> RFI Question A. (11):
>
> (11) Should OCR create exceptions or limitations to a requirement for covered entities to disclose PHI to other health care providers (or other covered entities) upon request? For example, should the requirement be limited to PHI in a designated record set? Should psychotherapy notes or other specific types of PHI (such as genetic information) be excluded from the disclosure requirement unless expressly authorized by the individual?

We offer two thoughts here. Making the administrative side of disclosure more complex will not help anyone. It will force more review and involve more lawyers than is warranted. If the rule provides for exceptions or limitations, then every request must go through an additional layer of review before a disclosure is possible.

A second observation is that genetics is increasingly part of normal, everyday medicine. Fueling genetic exceptionalism will interfere with the benefits that genetics brings to patients and to the health care system. Genetic information in a treatment context should be used and disclosed in the same way as other health care information. The need for rules covering genetic information arises when third parties outside the health care system use genetic information for other purposes, and that issue seems beyond the scope of the current RFI.

We further note that defining genetic information is a challenge, and that traditional definitions are not likely to work in a health care context. It will be too hard to pick and choose "genetic" information from other information with which the genetic information is integrated in a given health record. Asking for consent will be confusing to patients – who are generally not asked to consent to disclosures allowed by the HIPAA privacy rule – and burdensome to the health care system.

VI. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 13

> RFI Question A. (13):
>
> (13) Should individuals have a right to prevent certain disclosures of PHI that otherwise would be required for disclosure? For example, should an individual be able to restrict or ''opt out'' of certain types of required disclosures, such as for health care operations? Should any conditions apply to limit an individual's ability to opt out of required disclosures? For example, should a requirement to disclose PHI for treatment purposes override an individual's request to restrict disclosures to which a covered entity previously agreed?

In a comment on an earlier question (Section III in these comments), we noted the overly broad and overly vague definition for health care operations in the current version of HIPAA. It would be useful in HHS would find a way to narrow the definition and limit the ability of providers to use information virtually without restriction by calling the activity a health care operation. However, there does not seem to be any interest on the part of HHS in addressing this issue. That would be a narrower and better solution here.

We cannot imagine giving a patient a list of uses and disclosures that an institution makes under the rubric of health care operations and then allowing the patient to pick and choose which are allowable. Most patients will not understand what the activities are, and the most likely result is chaos, as patients make random choices allowing or disallowing some activities. Who is going to explain any of this to patients, and who is going to pay the cost of providing explanations?

HHS needs to impose realistic and narrow limits on the use and disclosure of patient records. Placing more responsibility on patients will not work. Frankly, we think that is unfortunate, but it is one of the realities of the modern world. Individuals do not have the knowledge, interest, or capability to engage in privacy management for their personal information held by dozens of third-party record keepers processing that information. It is an overwhelming task and most avoid it. Even those who are interested and informed find the gauntlet of privacy management options they face challenging.

Just to make the point clearer, an average family of four healthy individuals may easily have a dozen or more health care providers (GP, pediatrician, internist, dentist, pediatric dentist, gynecologist, hospital, urgent care practice, local pharmacy, mail order pharmacy, x-ray provider, laboratories, naturopaths, clearinghouses, etc.). Does HHS expect that patients will want to be involved in decision making about use and disclosure practices for all of these separate health care providers? It is inconceivable that patients could or would want to make all the required choices. The cost for covered entities in complying with patient choices would be enormous.

VII. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 17

> RFI Question A. (17):
>
> (17) Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard? For instance, should population-based case management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development be excepted from the minimum necessary requirement? Would these exceptions promote care coordination and/or case management? If so, how? Are there additional exceptions to the minimum necessary standard that OCR should consider?

The rule already makes the right balance by not applying the minimum necessary rule to disclosures to a health care provider for treatment. We are leery of any further weakening of the rule. The activities cited in this paragraph are vague and have no clear boundaries. If the minimum necessary rule is relaxed, then covered entities will do the convenient thing and share entire patient records with each other as they did before the rule took effect. The rule stopped that practice, and the technology is such today that sharing entire (or large parts) of a health record is much easier. If allowed, covered entities are likely to share all health records with each other and claim that it is for care coordination or some other unbounded activity. There will be central pools of health records that networks of providers will dip into as they see fit for care coordination, claims management, or what-have-you. The result will be a major hole in whatever privacy is left to patients under the rule, and the guarantee of an eventual data breach that will cover millions or tens of millions of people.

Industry, to be sure, would be happy to be freed from the obligation to pay attention and control what patient information it can share. What is convenient for industry is not good for patients, however. If there is no minimum necessary rule for these activities, then any type or extent of data sharing will be possible without any regard for privacy limits. We do not necessarily oppose all of the activities listed in paragraph 17, but we think that all of them can be done adequately with records that have been de-identified in some way. If a specific case can be made for loosening slightly the de-identification standards for some of the paragraph 17 activities, we might support that, but we would need to see an unambiguous factual basis for doing so.

We reiterate that we oppose weakening of the minimum necessary rule. We think that technology can provider better ways of accomplishing the purposes listed without exposing millions of patients to new privacy invasions. However, if HHS moves ahead with changes for any of the listed functions (or others) we suggest adoption of these balancing measures for any sharing of identifiable patient records:

1. Require each covered entity that discloses more than 50 patient records at one time for any of the listed functions post a notice on its website describing the number of records disclosed, the fields included in each disclosure, the recipient, the specific purpose of the disclosure, and the date when the records will be deleted by the recipient.

2. Prohibit any central pools of patient records or, in the alternative, require that each covered entity sharing records identify the name and location of the entity maintaining the records. Require the entity maintaining the records to identify itself publicly on a website and to list all covered entities providing patient records.

3. Impose strict liability on any covered entity that shared records with others for any health care operation purpose, with minimum liquidated damages for any breach or other improper disclosure of one hundred dollars per patient. Require the covered entity (and any entity maintaining a central pool) to maintain sufficient insurance to pay the liquidated damages to all patients.

4. Any records shared for a particular purpose must be deleted by the recipient when the purpose has been fulfilled or at the end of two years, whichever comes first.

5. Require the recipient of more than 50 patient records shared at one time for any health care operation purpose from a covered entity to take the burden of promptly removing from the records anything that is not essential for the purpose. In other words, impose the minimum necessary rule on the recipient rather than the discloser. Those required to take more responsibility for records they obtain may find that they don't need entire patient records after all.

VIII. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 18

> RFI Question A. (18):
>
> (18) Should OCR modify the Privacy Rule to clarify the scope of covered entities' ability to disclose PHI to social services agencies and community-based support programs where necessary to facilitate treatment and coordination of care with the provision of other services to the individual? For example, if a disabled individual needs housing near a specific health care provider to facilitate their health care needs, to what extent should the Privacy Rule permit a covered entity to disclose PHI to an agency that arranges for such housing? What limitations should apply to such disclosures? For example, should this permission apply only where the social service agency itself provides health care products or services? In order to make such disclosures to social service agencies (or other organizations providing such social services), should covered entities be required to enter into agreements with such entities that contain provisions similar to the provisions in business associate agreements?

What we see here is an attempt to eliminate the few remaining areas where patients have some right to control the sharing of their health records. We support the data sharing addressed for the types of activities listed in paragraph 18 ***provided that the data subject consents to the disclosure***. With consent, there is no issue about the need to have a business associate agreement, something that would be burdensome at best for everyone involved. That burden is the cost of eliminating patient consent. This is, in many ways, the same problem addressed elsewhere, where HHS invites industry to complain about existing privacy protections that are inconvenient for covered entities but that protect patients.

We observe that social service agencies are subject to a welter of different privacy regimes, and in some or many cases, no privacy regime at all. If HHS combines more non-consensual disclosures with relaxation of the minimum necessary rule, records shared with some social service institutions could be further shared in whole or in part without any restriction at all. Business associate agreements can restrict that further disclosure and would be better than nothing, but the administrative burden on everyone involved would be enormous.

In this case, consent cures the problem in a better and less costly way. Patients can speak for themselves and protect their own interests. We already see too much in the RFI that undermines

patient rights in the interest of convenience for institutions. We recognize that there can be a need for a tradeoff at times, but the RFI is not balanced: it appears to be heaving so far to one side as to capsize the patient privacy ship entirely.

IX. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 19

> RFI Question A. (19):
>
> (19) Should OCR expressly permit disclosures of PHI to multi-disciplinary/ multi-agency teams tasked with ensuring that individuals in need in a particular jurisdiction can access the full spectrum of available health and social services? Should the permission be limited in some way to prevent unintended adverse consequences for individuals? For example, should covered entities be prevented from disclosing PHI under this permission to a multi-agency team that includes a law enforcement official, given the potential to place individuals at legal risk? Should a permission apply to multi- disciplinary teams that include law enforcement officials only if such teams are established through a drug court program? Should such a multi- disciplinary team be required to enter into a business associate (or similar) agreement with the covered entity? What safeguards are essential to preserving individuals' privacy in this context?

Question A 19 is unfocused, and therefore confusing. The rule already allows disclosure to law enforcement with little more than an oral request. The idea in paragraph 19 seems be to expand sharing of patient information to "multi-disciplinary teams" that would include law enforcement. In other words, the proposal would potentially expand non-consensual law enforcement access to records and place patients at greater jeopardy for privacy loss and place them in additional legal jeopardy for any potential criminal conduct disclosed to their health care provider.

We assume that the goal here is to improve response to the opioid crisis, and we are not entirely unsympathetic to that goal. However, we see paragraph 19 as opening the door to turning the health care system into a general surveillance system for law enforcement. Today it might be the drug crisis, but tomorrow it could be for immigration violations, parents who skip child support payments, or another crime of the week.

It is not clear to us how to limit any expanded sharing just to drug abuse situations. Without clear and specific limits here, every potential crime disclosed to a health care provider could be fair game for some enterprising "multi-disciplinary team." We suggest that the only answer here is to rely on consent for disclosures. If there is a drug court involved, the court can help to obtain patient consent. If a court has the ability to impose an order allowing data sharing, the rule already allows that.

We do not see a business associate agreement as helpful here. It would be a burden for all involved, and it would not provide any real protections for patients. Would anyone be willing the make a patient a third-party beneficiary of a business associate agreement so that patients would

have at least some remedy if their records were used in violation of the agreement? We doubt that very much, although we would welcome a general addition to the rule that accomplished that purpose generally.

If the rule required some type of exclusionary rule for some law enforcement uses of the information, we do not see how that rule could be enforced. Does HHS have the jurisdiction to determine what evidence can be used in investigations or in court for all law enforcement agencies and for all courts throughout the United States?

We note that a little known Executive Order from 2000 (E.O, 13181, To Protect The Privacy Of Protected Health Information In Oversight Investigations, https://www.gpo.gov/fdsys/pkg/FR-2000-12-26/pdf/00-33004.pdf) provides some protection for use of patient records in law enforcement activities. In general, it seeks to stop the use of protected health information concerning an individual that is discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations of a non-health oversight matter. This Order is not of great relevance in opioid cases, but we point it out for a specific reason. The Order applies only to the federal government. **The President could not impose restrictions on state and local law enforcement use of HIPAA protected records. We do not think that HHS can do it either, whether by rule or though business associate agreement.**

We do not see how HHS can write the rule to allow disclosure to teams including law enforcement and set the terms under which those teams operate. HHS has not claimed jurisdiction over recipients of PHI who are not themselves subject to the rule. We do not see how it could do it here.

X. Questions on topic A, Promoting Information Sharing for Treatment and Care Coordination, Question A. 20

> RFI Question A. (20):
>
> (20) Would increased public outreach and education on existing provisions of the HIPAA Privacy Rule that permit uses and disclosures of PHI for care coordination and/or case management, without regulatory change, be sufficient to effectively facilitate these activities? If so, what form should such outreach and education take and to what audience(s) should it be directed?

We do not oppose public outreach and education as a general policy. But any efforts under HIPAA for this specific purpose must compete with other similar efforts under HIPAA, efforts under other privacy laws, and efforts to educate consumers about computer security, tire pressure, nutrition, retirement savings, and an untold host of other issues. After all these years, patients (and providers) still do not understand the goal of the form a patient is asked to sign when they visit a provider. There is virtually no hope that public education will meaningfully help here. Even if it did, how would educating the public make a difference if HHS changed the rule to expand non-consensual disclosures?

XI. Questions on topic B, Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness

> RFI Questions B 22-26:
>
> B. Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness

We will not go through the questions raised here individually, we will address the question broadly. We recognize the public concerns and the political reaction to those concerns that prompted Part B of this RFI. This is an area where hard cases have the potential to make bad law.

In our view, the privacy rule already strikes a good balance with respect to disclosures to parents and other caregivers. The flexibility and the discretion given to health care providers seems to have worked well in most cases. Especially in cases involving children, where the balances involved are delicate, and the rule reasonably leaves some of those balances to state law.

It is unfortunate that some people make bad choices or have bad results with their lives, whether through their own fault or through no fault of their own. Students drop out of school, individuals make bad investments, fail to save for retirement, go bankrupt, drive unsafely, drink too much alcohol, etc. We would welcome a reasonable way to avoid these unfortunate results as much as anyone.

Undermining privacy rules that apply to all will not solve the problems of opioid addiction or mental health. **The risk – and it is a great risk – is that changing the rules will make the health care system work less well because individuals will lose confidence that they can talk to their doctors.** Sharing more information with relatives may help in some cases, but there may be just as many cases in which the possibility of information sharing may dissuade individuals from seeking or accepting help. Educating providers so that they know how much ability they have under the privacy rule is helpful, and HHS already took action in this regard. We conclude that this may be the best result for all, even if a different process might benefit a few at greater cost to others.

XII. Questions on topic C, Accounting of Disclosures

> RFI Questions C. (27-42):
>
> C. Accounting of Disclosures

We recognize the complexity of accounting for disclosures. We also recognize the value of accounting. There are so many non-consensual uses and disclosures of health records that an accounting for disclosures is the only way that a given patient can find out what happened to their record. It is the only accountability measure available to patients.

We also observe that in many cases, hospitals now have electronic systems in place that are capable of tracking all uses and accesses by staff. Numerous news stories reported on hospitals that disciplined staff members for peeking at records of patients (often records belonging to celebrities) when the staff members have no business accessing the records. These hospitals can find who looked at the record, with time stamps and numbers of accesses. Providers therefore are also able to make those records available to inquiring patients.

HHS should take a new and different approach to accounting based on two simple principles. First, if a covered entity has a system that tracks accesses and disclosures of a patient record and that tracking can be readily retrieved, then it must be shared with inquiring patients. We do not see any reason to draw distinctions between use and disclosure if covered entities have problems with those concepts. If a covered entity cannot distinguish, then its accounting can include the name, date, and purpose of all accesses and all disclosures. But its obligation today should be to share what it has with patients who ask. If accounting records are partial today, then so be it.

Second, if a covered entity does not have a system for tracking all accesses and disclosures of a patient record, then it must adopt one when it next upgrades its computer system in a major way or in the next ten years, whichever comes first.

Covered entities need to know for their own purposes who is using patient records. To some extent, they already established the capability of complying with the accounting requirement in the existing rule. We want to see the requirement expanded, but it does not matter that much how long it will take to accomplish that expansion. Technology can and will keep track of all uses and disclosures. Covered entities will want that capability for their own purposes. If HHS imposes the requirement, then vendors will include the capability in their next upgrades. Make it ten years if you must, but give patients today what is available today, and make covered entities do more without requiring them to retrofit their existing systems at great expense.

XIII. Questions on topic D, Notice of Privacy Practices, Question 52, regarding modifications to the NPP

> RFI Question D. (52):
>
> (52) Are there modifications to the content and provision of NPP requirements that would lessen the burden of compliance for covered entities while preserving transparency about covered entities' privacy practices and individuals' awareness of privacy rights? Please identify specific benefits and burdens to the covered entity and individual, and offer suggested modifications.

In general, HHS asks whether the collection of a signature signifying acknowledgement of receipt of a notice of privacy practices is a good idea. In our view, the requirement to collect a signature was a poor choice in the first place. In practice, the requirement failed to achieve any benefits at all.

First, few patients understand what the signature means. Patients think that the signature means that they are agreeing to the use and disclosure of their record. This was the practice in the years before HIPAA, when any health care encounter was accompanied by the signature of a form that gave the provider the right to use and disclose the patient's information for virtually any purpose. Patients signed those forms without understanding what they were signing. The health care system at the time could not accommodate variations, and patients who modified the forms were ignored. The process served to protect providers and actually harmed patients by forcing them to agree to overly expansive and often unbounded uses and disclosures of their records. By replacing that system, HIPAA did a backhanded service to patients. Whether the expansive non-consensual disclosures otherwise allowed by the rule helped or hurt patients more is an issue that we leave without further debate here.

Second, patients sign the HIPAA acknowledgement form without understanding the purpose or meaning of the form. Luckily, there is virtually no meaning to the acknowledgement form so patients are not harmed as a result. In that regard, HIPAA was an improvement, but only because it replaced a practice harmful to patients with a meaningless one.

Third, few providers understand what the signature means. Perhaps the lawyer responsible for privacy or the covered entity's privacy officer understood the process. However, the receptionists in most medical offices did not understand. They often told patients that they had to sign the form or they could not see the provider.

Fourth, patients who sign the acknowledgement form often did not actually receive a copy of the NPP. In fact, a patient who signed the form and actually asked for a copy often received a blank state from an uninformed receptionist. The signature and the distribution of an NPP were not related events in the eyes of most reception desks. The acknowledgement from the patient was not true. We have asked for an NPP when handed the form and were told it was not available, but we should sign the form anyway.

In short, the signature accomplished little and at significant cost. We support ending the requirement for a signed acknowledgement for the receipt of an NPP. However, we strongly oppose allowing health care providers to collect any signature from patients when they walk into a health care providers office. With one exception explained below, we recommend that HHS expressly ban the practice of asking patients to sign a form when they arrive at the office of a health care provider. We do not want HHS to allow a signature "void" to be replaced by the signing of a new form that providers can use to accomplish some purpose not likely to benefit patients. We do not want provider to use the "opportunity" to collect new authorizations from patients. If HHS removes the acknowledgement requirement, then it should expressly ban any collection of patient authorizations at patient intake in a health provider's office.

When adopting the HIPAA rule, HHS extended the old practice of patients signing forms and trained a new generation of patients with the expectation that they must sign something in order to see a health care provider. That must end. It never benefitted the patient, and it never will. We need to retrain patients *not* to sign forms, even if it takes thirty years to work.

The only exception that we acknowledge is the practice of a sign-in sheet. These sign-in sheet record the time of arrival of patients and are often used by providers to account for each patient seen. We do not like sign-in sheets, but we do not object provided that the signature on a sign-in sheet is nothing more than a statement of presence. It should not also be treated by the provider to be agreement to a disclosure authorization or to anything else. HHS should expressly state that a sign-in signature may not have any substantive meaning.

In the early days of HIPAA, many offices used improper sign-in sheets that allowed each subsequent patient to see who came before and, in some cases, which doctor that patient saw. These disclosures expressly violated the rule by exposing patient information to their friends and neighbors. In our experience, health offices today have improved their policies and found a way to remove each patient signature from the sign-in form so that it was no longer accessible by later patients. It took a long time for that practice to take hold, and we do not know for sure that the old practice is entirely gone. It is clear, however, that things have improved somewhat. We suggest that HHS consider providing express guidance to covered entities on the proper use of sign-in sheets just to help further.

The broader problem raised by HHS is how to educate patients about their rights under HIPAA. The signature on an acknowledgement form did not work. We admit that educating patients is a hard problem. We noted elsewhere in these comments that the market for educating consumers is vast, even if we limit the scope to the market for accurate and useful information. If we also consider those who want to "educate" consumers in order to cheat them, that market is even bigger, and the odds of a needed message getting through to a willing consumer are even smaller.

Handing out NPPs may help a few consumers. Posting NPPs will help a few. Other methods may help too. But you cannot make consumers read forms and you cannot make them understand the forms without great efforts. In the context of an average health care encounter, there is no real opportunity for great efforts on privacy education. We do not oppose educational activities, but we recognize that most efforts will fall on infertile grounds.

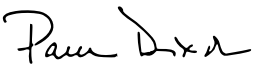
Our view, and we practice what we say here, is that it is important to make information that patients need available to them when they discover that they need that information. We provide a ***Patient's Guide To HIPAA*** on our website that allows patients to find answers to their health privacy questions when they go the Internet to look. There are few websites that provide patients with the advice that they need. We are pleased that our HIPAA resource receives a significant amount of traffic. See: https://www.worldprivacyforum.org/2013/09/hippaguudeindex/.

XIV. Conclusion

We thank you for the opportunity to submit these comments. We encourage HHS to reach out to us for additional comments or questions; some of the proposals in the RFI are of great concern, and would greatly weaken patient privacy. We are interested in ensuring that patients can continue to rely on the existing protections in HIPAA. In this time characterized by debilitating data breach and meaningful loss of trust in electronic systems, it is absolutely crucial for the HIPAA privacy rule and security rule to remain as strong as possible. Weakening privacy today

sends exactly the wrong message to people who are already concerned about the breaches they see in the system. We can all do more to protect and advance patient privacy, and we all must do better.

Respectfully submitted,



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