Comments of the World Privacy Forum

Regarding: Department of Health and Human Services, Office for Civil Rights, Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended, RIN 0945-AA04

Sent via https://www.regulations.gov

Attention: HITECH Act Recognized Security Practices
Request for Information, RIN 0945–AA04
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue SW
Washington, DC 20201

June 3, 2022

The World Privacy Forum welcomes the opportunity to respond to the Request for Information from the Office of Civil Rights of the Department of Health and Human Services titled *Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended*. The RFI appeared in the Federal Register on April 6, 2022, at https://www.federalregister.gov/d/2022-07210.

The World Privacy Forum (WPF) is a nonprofit, non-partisan 501(c)(3) public interest research group. WPF focuses on multiple aspects of privacy, with health privacy being among our key areas of work. We publish a large body of health privacy information, including guides to HIPAA; reports and FAQs for victims of medical identity theft; and materials on genetic privacy, precision medicine, electronic health records, and more. We testify before Congress and federal agencies, and we regularly submit comments on HIPAA and related regulations. WPF's Executive Director co-chairs a Research, Academic, and Technical working group at the World Health Organization (WHO) and is engaged in multiple aspects of health data ecosystems and their governance and privacy. For more about our work and our reports, data visualizations, testimony, consumer guides, and comments, see http://www.worldprivacyforum.org.

In general, the RFI did an excellent job in identifying the complex issues raised by sharing penalties assessed by the Office of Civil Rights (OCR) under HIPAA with individuals harmed by noncompliance with HIPAA rules. The statute presents OCR with a multitude of challenges. Defining harm and deciding how to award compensation to harmed individuals is not a simple task.

Our comments focus on two areas: first, conflict of interest issues, and second, determining harms.

1. Conflict of Interest

The statute provides that:

> ...any civil monetary penalty or monetary settlement collected with respect to an offense punishable under this subchapter or section 1176 of the Social Security Act (42 U.S.C. 1320d–5) insofar as such section relates to privacy or security **shall be transferred to the Office for Civil Rights of the Department of Health and Human Services to be used for purposes of enforcing the provisions of this subchapter and subparts C and E of part 164 of title 45**, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009. 42 U.S.C. 17939(c)(1), https://www.law.cornell.edu/uscode/text/42/17939.

We bolded the language that raises the issue we address here. We want to state clearly that the conflict of interest problems we discuss here are the result of the way that Congress drafted the legislation. Congress did not provide sufficient guidance or direction regarding conflict of interest issues before requiring HHS to craft a methodology to solve the problem. The problems are not the result of actions taken or not taken by the Department. Nevertheless, it is incumbent on the Department to address the problem in a reasonable way.

The statute provides that penalties assessed under the HIPAA enforcement process be given to OCR to be used for enforcement of HIPAA. By itself, this provision raises a modest conflict of interest in that OCR can keep penalties to enhance its budget. We cannot assess the extent to which this provision has influenced the penalties imposed to date. Over the years, actual practice has varied widely, ranging from few or no penalties in the beginning, large penalties during a second phase of enforcement, and smaller penalties more recently.

Another provision calls for penalty sharing:

> (3) Establishment of methodology to distribute percentage of CMPS collected to harmed individuals
>
> Not later than 3 years after February 17, 2009, the Secretary shall establish by regulation and based on the recommendations submitted under paragraph (2), a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil

> monetary penalty or monetary settlement collected with respect to such offense. 42 U.S.C. 17939(c)(3), https://www.law.cornell.edu/uscode/text/42/17939.

The current effort to implement the "penalty-sharing" part of the statute raises the conflict-of-interest problem to another dimension. It is one thing for the Department to assess and keep the penalties imposed for violations. It is another matter for the Department to decide how to share the penalties with others. To state the matter in clearer terms, the statute directs OCR to serve as investigator, prosecutor, judge, and jury, and then to decide how to share the resulting penalties between its own budget and those individuals who were harmed by the violations of law. This is a nearly impossible situation for anyone. No matter how the Department acts in any particular case, it can easily be criticized from multiple different directions.

We note that the statute directed HHS to act to share penalties with individuals by February 17, 2012. That date was over ten years ago. Only now did HHS take the first step toward implementing the penalty sharing by issuing an RFI. Future steps may include an advance notice of proposed rulemaking and then a notice of proposed rulemaking and then an actual rule. This process could easily take many more years before actual implementation of the congressional directive. One could easily conclude that HHS dragged its feet, while keeping the penalties assessed for OCR's budget.

This is the type of conclusion that can readily follow when there is an inherent conflict of interest. We want to make it clear, however, that we make no accusations in this matter. We recognize that there are many factors that go into rulemaking activities and that delays in meeting statutory deadlines are common. Nevertheless, it is too easy to look for nefarious motives. Everything that HHS and OCR does in this space can be questioned through a conflict-of-interest lens.

HHS needs to find a way to separate some of the choices that arise when deciding how to divide up collected penalties. We believe it is important that, to the greatest extent possible, the Department should establish rules and procedures to guide the penalty sharing that avoid conflict-of-interest issues to the greatest extent possible. We offer a variety of ideas here.

First, in theory, the Department could avoid all conflict issues by providing that all funds go to victims and none to the Department. Unfortunately, in some cases, there may be large numbers of victims and not enough money to distribute as a practical matter. Administrative costs of distribution must be considered. Consider a data breach that affects 500,000 individuals. If the penalty is one million dollars, that is two dollars per individual. The administrative costs would consume all funds and then some. Even if the Department tried to focus the funds on those who could demonstrate harm, the cost of the determinations could consume all funds as well. Imagine adjudicating 25,000 individual claims. We reluctantly conclude that a victim-only rule simply will not work in all cases. This is likely to be true even before we reach the challenging problem of assessing individual harm.

This leads us to suggest a procedural method of avoiding conflicts. If the Department designated or hired a neutral third party to decide how to allocate the penalties, the Department would come much closer to avoiding conflicts of interest. That third party could be an administrative law

judge, an arbitrator, a mediator, or a neutral third party hired for the purpose. The most important job of the third party may be to make an initial decision about allocating penalties between the Department and victims. For that reason, it would be essential that any decision maker have no ties to the Department. The appointment of the third party should be for a term of a set number of years without the possibility of renewal.

It is likely that some basic rules will be useful for whomever makes allocation decisions, whether that be a board, a group, or a third party. For example, when a penalty has resulted from a case where an individual complained about denial of access to records, the complaining individual could be compensated for the effort of pursuing the records and filing the complaint. If a denial resulted in additional expenses (e.g., duplicate testing) or worse outcomes (delayed diagnosis), additional compensation should be allowed. Even this simple case is not easy. We recognize that the costs of duplicate testing may not always be borne by the individual. There may be health insurers who paid for the tests. There could be other remote victims as well. Denial of records could increase costs for employers. A family member and not the actual data subject may have expended time and effort to obtain the patient's record. It may be that there is a need for a rule that compensation is only available for direct harms to a patient.

We think that it will take more work to develop rules that are fair and that avoid or limit the conflicts of interest inherent in the statutory requirement for penalty sharing. What we suggest here is just a start.

2. Determining harm

The RFI states:

> ...the term ''harm'' is not defined by statute, and the HITECH Act does not provide HHS direction in how to define harm. Rather, the only qualification is that a relationship exists between the harm and the act of noncompliance with the HIPAA Rules. The Enforcement Rule identifies four types of harm as mitigating and aggravating factors that may be considered in determining the amount of CMPs—physical, financial, reputational, and ability to obtain health care—while leaving open the possibility of other types of harm.[31] [32] However, the Enforcement Rule does not specifically define each of those types of harms, and the HITECH Act does not require OCR to apply those exact same harms to a methodology for distributing a percentage of CMPs and monetary settlements to harmed individuals. Therefore, OCR is considering what harms may make an individual eligible to receive such distributions.

Determining harm in the health care context is a complex matter, and harms in the health sector can result from a myriad of factors and interactions. Not all harm is of equal importance--we note that there is a distinct continuum of harms that HHS could map out. Harms can range from straightforward non-compliance, for example, a covered entity's refusal to provide an accounting of disclosures, to more serious harms such a refusal of record sharing that leads to a late diagnosis, leading to poor medical outcomes. As a general overview of thinking regarding harms, we recommend that the Department read and consider a new law journal article relevant to the problem. Danielle Keats Citron and Daniel J. Solove recently published *Privacy Harms*, 102

Boston University Law Review 793 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, This article represents the best of current thinking on the problem of identifying privacy harms that are appropriate for compensation.

We note that there are harms that can occur from aggressive and persistent bad actors, who manage to break the defenses of even the most HIPAA-compliant entities. This raises a number of challenging issues. One issue we would like to specifically raise in this context is medical identity theft. Medical identity theft is a specific category of harm that WPF urges HHS to take into serious consideration.

WPF is extremely familiar with this particular crime, and the serious harms it creates, which can include both financial and medical harms. In 2005, WPF was asked to testify about the risks of the then-proposed National Health Information Network (NHIN) before the National Committee on Vital and Health Statistics (NCVHS.) In our testimony, we discussed - for the first time on public record - what we termed "medical identity theft." (*Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environments,* http://www.worldprivacyforum.org/wp-content/uploads/2005/08/pamdixonNCVHStestimonyfinal.pdf) In 2006, we published the first major report on medical identity theft in which we defined the term, documented the harms, the scope of the crime at the time, and documented the modus operandi of the crime and provided recommendations. (Pam Dixon, Robert Gellman, *Medical Identity Theft: The information crime that can kill you*, https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/) In subsequent years we have created a great deal of material around medical identity theft, including FAQs for victims, and we created a methodology with health care providers to help in mitigating the errors in medical records that is one of the terrible hallmarks of this crime. See WPF's dedicated medical identity theft page with medical identity theft research and resources: https://www.worldprivacyforum.org/category/med-id-theft/.

We have received many requests for assistance from victims of this crime, which is why we know that this crime can have devastating consequences with the potential to impact patients for years. Some never fully recover the integrity of their health files, depending on the provider. Some never fully recover financially, and some have suffered other terrible consequences - people have had their children removed from their care for months due to medical ID theft, people have received improper care based on file errors introduced by fraudulent actors, people have had hospital bills in multiple states for expensive surgeries they never had, and some have had problems getting a job due to incorrect information placed fraudulently in their medical file.

Today, medical identity theft is now a known and acknowledged problem, and although we have made great strides in preventing and solving the problems that this crime poses, medical identity theft still exists, and there are still victims who are suffering in some cases significant, wide-ranging harms. We encourage the Department to specifically acknowledge medical identity theft as a crime that creates a range of consequential harms for many of its victims.

Regarding the intersection with HIPAA, some medical identity theft has resulted from non-compliance. But not all medical identity theft has resulted from straightforward non-compliance. We acknowledge the complexity involved in determining whether a covered entity was compliant or non-compliant with HIPAA regarding medical identity theft crimes. We urge the Department to clarify the interactions of medical identity theft in regards to the health care sector vis à vis HIPAA compliance or non-compliance. There is very little guidance regarding what specifically HIPAA compliance means in the context of this crime.

One thing that is not opaque, however is the extensive range of harms involved in medical identity theft, which has now been documented for 17 years and counting. We urge the Department to provide clarity for the victims of this crime. As mentioned, medical identity theft is a serious crime, and both patients and providers need a clearer roadmap for handling the full lifecycle of this crime, from the inception all the way through to the aftermath, which will hopefully include redress that will make the victims whole in as much as is possible.

We thank you for the opportunity to offer these comments, and we stand ready to assist.

Respectfully submitted,

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