Comments of the World Privacy Forum

To the Department of Health and Human Services

Regarding RIN 0991–AB56, HITECH Breach Notification

Via regulations.gov and email

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, SW.
Washington, DC 20201

October 23, 2009

Re: HITECH Breach Rule, RIN 0991–AB56, 74 Fed. Reg. 42740-42770.

The World Privacy Forum appreciates the opportunity to comment on the Department of Health and Human Services's Interim Final Rule on Breach Notification for Unsecured Protected Health Information. The rule appeared in the Federal Register on August 24, 2009 at 74 Fed. Reg. 42740-42770.

The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, in particular issues related to information privacy, health privacy, and financial privacy. More information about the activities of the World Privacy Forum is available at our web site, <http://www.worldprivacyforum.org>.

We have a number of concerns and suggestions regarding the proposed interim rule, which we discuss in more detail below.

I. Unintentional or Inadvertent Disclosures

A breach notification rule has to strike a fair balance between three overlapping and partially conflicting realities. First, the cost and consequences of notification to the record keeper can be

significant, although we have little sympathy for record keepers responsible for avoidable breaches. Second, the value of notification to victims can be limited, but notification still has a value both for victims and for its deterrent effect. Third, the need to allow victims of a breach to take actions to protect themselves and their privacy cannot be dismissed lightly.

One of the goals of breach notification is to allow victims to take steps to monitor or avoid identity theft. We observe that there are significant differences between medical identity theft and financial identity theft on this score. Please see our 2006 report on Medical Identity Theft, *Medical Identity Theft: The Information Crime that Can Kill You* <http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>. We will also be publishing an extensive new report on medical identity theft in January 2010. We have learned a great deal about medical identity theft in researching our reports on the topic. Some of the steps that a potential victim of financial identity theft can take are not likely to be of significant value to a potential victim of *medical* identity theft. For example, credit monitoring is not likely to reveal medical identity theft at all or only after a significant delay. We will return to this point about the content of a medical breach notification later in these comments.

Making the choices about breach notification is an exercise in making tradeoffs. The legislation sought to limit notification in cases where breaches were unintentional or inadvertent and no consequence likely followed. The lesson that the Department of Health and Human Services (HHS) should have drawn from the statutory exceptions to the breach definition is that Congress intended to focus on *external disclosure*. HHS has not paid enough attention to this message. Instead, HHS decided to make it procedurally cumbersome for a covered entity to decide that an unintentional or inadvertent action falls under an exception.

Our concern arises in § 164.414(b) of the rule, which provides:

> In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or **that the use or disclosure did not constitute a breach**, as defined at § 164.402.

As a privacy group, the World Privacy Forum supports a fair implementation of the statute, with an appropriate emphasis on the privacy of victims of security breaches. At the same time, we recognize that resources available for privacy are limited. Our concern here is that HHS has written the rule in a manner that will require the unnecessary expenditure of resources that will not benefit data subjects or their privacy.

Many health care institutions handle large volumes of patients, sometimes under emergency conditions where choices are made that may have immediate consequences for life or health. Even in the absence of emergencies, the necessity of seeing large numbers of patients under time constraints creates its own pressures. We don't seek to excuse mistakes by covered entities. However, we recognize that unintentional or inadvertent actions wholly within a health care institution and among its workforce will occur with some regularity. These actions occur regularly in non-health circumstances as well. Any organization dealing with large volume of people and records will expose records improperly from time to time.

With this in mind, we turn to the implementation procedure that HHS envisions is set out on page 42748 of the Federal Register.

> **With respect to any of the three exceptions discussed above, a covered entity or business associate has the burden of proof**, pursuant to § 164.414(b) (discussed below), for showing why breach notification was not required. **Accordingly, the covered entity or business associate must document why the impermissible use or disclosure falls under one of the above exceptions.**
>
> Based on the above, we envision that covered entities and business associates will need to do the following to determine whether a breach occurred. First, the covered entity or business associate must determine whether there has been an impermissible use or disclosure of protected health information under the Privacy Rule. **Second, the covered entity or business associate must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the protected health information.** This occurs when there is a significant risk of financial, reputational, or other harm to the individual. Lastly, the covered entity or business associate may need to determine whether the incident falls under one of the exceptions in paragraph (2) of the breach definition.

We highlighted a few sentences from the rule. These sentences make it clear that a covered entity that has an unintentional or inadvertent breach will be required to undertake an administrative process that will 1) be complicated, disruptive, and expensive; 2) not be a rare event; and 3) frequently result in no application of the breach notification requirement.

We do not believe that the process set out by HHS is realistic or, more importantly, is a wise use of resources. HHS's own example from page 42747 makes the point:

> A billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it. The billing employee unintentionally accessed protected health information to which he was not authorized to have access. However, the billing employee's use of the information was done in good faith and within the scope of authority, and therefore, would not constitute a breach and notification would not be required, provided the employee did not further use or disclose the information accessed in a manner not permitted by the Privacy Rule.

We agree with the result suggested here. However, the process that the covered entity would be required to follow to determine and document the error is a significant burden. A misdirected email that was sent to an entire department rather than to one individual could require a major investigation in order to meet the determination and documentation standard that HHS requires.

It would be necessary to contact each recipient and to find and document facts about the use or further disclosure of the information.

The requirement to document unintentional or inadvertent actions internal to a covered entity is too burdensome. We propose that the requirement be dropped for actions that are internal to a covered entity (including business associates). The obligation to determine and document should apply only when there is some actual reason to believe that there is a likelihood of harm as a result of disclosure outside the covered entity. A covered entity can be required to train its workforce to recognize these circumstances. The workforce is already trained in HIPAA, and everyone should know what the rules are with respect to identifiable health information.

The focus in the rule should be much more on the possibility and consequence of disclosures outside the covered entity. These disclosures present the greater threat to patients. Generally speaking, outsiders are not as likely to know what the privacy rules are, and they are likely to have no obligation to patients.

In saying this let us clarify that we are very aware that bad actors on the inside of the health care system exist. For example, snooping by hospital employees – especially in cases involving celebrities – is a significant problem. So is the abuse of insider access to patient records, such as what has happened in troubling cases where patient information has been sold.[1] However, we believe the breach notification rule is the wrong place to fight this battle. Unfortunately, in the HIPAA privacy rule, HHS did not require accounting for all ***uses*** of health records, and that mistake makes it hard to track snooping. Luckily, some institutions have computer systems that track uses by staff, and these systems, when used correctly and with oversight, have provided the evidence necessary to support disciplinary actions and to curb the insider threat.

We support narrowing the determination and documentation requirement for internal actions because we want to focus scarce resources more on those actions that will have serious consequences for victims. Unintentional or inadvertent actions wholly within a clinical or billing setting should fall outside the requirement for determination and documentation without additional evidence that a problem is likely to arise.

II. Risk Assessment

On the other hand, we want better procedures and assessments when serious breaches occur. The risk assessment provisions described (page 42744) by HHS are not adequate.

> Thus, to determine if an impermissible use or disclosure of protected health information constitutes a breach, covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In performing the risk assessment, covered entities and business associates may need

[1] See for example the Machado-Ferrer case where 1,500 Cleveland Clinic patient records were sold by an employee. See <http://www.usdoj.gov/usao/fls/PressReleases/080401-01.html>. See also <http://www.usdoj.gov/usao/fls/PressReleases/Attachments/080401-01.Chart.pdf>.

> to consider a number or combination of factors, some of which are described below.

We have several suggestions.

First, the requirement for a risk assessment should be *expressly stated* in the rule itself and not just in the description accompanying the rule.

Second, in some or all cases, HHS should require that the risk assessment be conducted by an independent organization. We are concerned that an assessment conducted by a component whose budget may be charged with the cost of notification will not provide a fair evaluation. The requirement for an independent risk assessment might be limited to breaches that involve large numbers of records or particular classes of information (e.g., SSNs, medical insurance numbers, credit card or bank account information, or PHI covered by specific additional confidentiality requirements, such as substance abuse, mental health, AIDS, or genetic information). We wonder in passing whether there might be a role for patient safety organizations in conducting these risk assessments, although there should be no reason to treat risk assessments as privileged as is the case with safety information.

Third, even if risk assessments are conducted by independent organizations, we are concerned that there will be a race to the bottom as risk assessors compete to find that a breach creates no risk of harm. A covered entity might well be tempted to hire the least rigorous risk assessor unless there are some standards that must be met. **We suggest that HHS publish risk assessment standards or model risk assessments so that covered entities will have specific examples to guide their own activities.**

Fourth, the best way to induce covered entities to do a reasonable risk assessment is for HHS to commit to conducting random audits of risk assessments. If covered entities know that there is some prospect that their risk assessments will be reviewed and that they will be held accountable for their implementation of the requirements, they will likely to a better job.

III. Notification Content

The rule requires that the notification sent to victims of a breach describe:

> (C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

This is inadequate direction for the content of a notification. Depending on the circumstances and content of the breach, there may be more than a dozen steps that a victim would be well advised to take, as well as some steps that a victim would be advised not to take. The World Privacy Forum expects to publish shortly a list of things that potential victims of medical identity theft (and that may include many victims of security breaches) should take and should not take. We repeat the observation above that credit monitoring is not likely to reveal medical identity theft at all or only after a significant delay. Credit monitoring may be useful if a breach may increase the likelihood of financial identity theft, but it is not likely to help to uncover all cases

of medical identity theft. Health care institutions that expose patients to a risk of medical identity theft should not be allowed to get by simply by offering non-responsive credit monitoring to victims of a breach.

Rather than leave every institution that experiences a security breach to reinvent the wheel and decide for itself what steps individuals should take to protect themselves, HHS should publish its own list and require that its current list of actions be included in each notification. It is likely that more than one list would be needed because the type of information improperly disclosed will affect what steps should be taken by consumers. For example, if the breach involved name, address, and SSN, actions to be taken should include the more familiar steps for monitoring and avoiding financial identity theft. If the breach included name and health insurance number, the actions to be taken should focus on monitoring and avoiding medical identity theft.

HHS can do a better job in providing more specific guidance on the content of breach notification. Based on the history of breach notification at the state level, we see that specific guidance on notice content can be helpful for both the institution that had the breach and those notified. See for example the California Office of Privacy Protection's Breach Notification booklet for businesses at:<http://www.oispp.ca.gov/consumer_privacy/pdf/COPP_Breach_Reco_Practices_6-09.pdf>.

The World Privacy Forum appreciates the opportunity to offer these comments.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org
760-268-0096