Comments of the World Privacy Forum regarding HITECH Act, Section 13402 Guidance and Request for Information

to

Office of the Secretary, Department of Health and Human Services

Via www.regulations.gov

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

May 21, 2009

Re: Proposed Guidance and Request for Comments under §13402 of the HITECH Act, at 74 Fed. Reg. 19006-19010.

The World Privacy Forum appreciates the opportunity to comment on the Department of Health And Human Services' proposed guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals for purposes of fulfilling the breach notification requirements under §13402 of the HITECH Act of the American Recovery and Reinvestment Act of 2009 (ARRA). The proposed guidance and request for comments appeared in the Federal Register on April 27, 2009 at 74 Fed. Reg. 19006-19010.

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 and health privacy. More information about the activities of the World Privacy Forum is available at our web site, <http://www.worldprivacyforum.org>.

Our comments focus primarily on issues relating to *limited data sets* and breach notification.

I. Comments Regarding Breach Notification and Limited Data Sets

The question of whether to include *limited data sets*[1] as part of breach notification presents substantial difficulties. No matter which decision HHS arrives at -- to include limited data sets as part of breach notification or to exclude limited data sets from breach notification -- there are privacy compromises on each side of the decision. Our comments briefly outline some of the more significant issues, and suggest some potential middle ground.

There are privacy interests in limited data sets, as the HHS proposed guidance notes.[2] Among the greatest risks is that of re-identification, with the potential for unanticipated and unauthorized secondary uses. As technologies have matured and computing power has increased, the risk of re-identification of information contained in limited data sets is no small matter.

If individual breach notices *are not* required for limited data sets, individuals with a privacy interest in the data could be excluded from knowing about potential re-identification problems. If the sets *are* included in individual breach notice, in order to notify, the data will have to be re-identified, which is problematic for individuals' privacy interests. The original design of the limited data set option in the HIPAA rule sought to avoid any re-identification by the recipient. Breach notification of individuals will conflict with that goal and, indeed, with the original premise of limited data set disclosures.

Additionally, many individuals who are notified of a breach will be confused about why the limited data set user had the data in the first place. For example, in a breach of a limited data set being used for research, an individual would first have to be re-identified in order to send a breach notice, then notified. That individual is unlikely to know prior to receiving notice that a limited data set was lawfully used for research purposes. The re-identification of individuals in a limited data set and delivering notice will create its own set of records at the data source, at the limited data set user, or possibly a third party. Whatever the status of those records under the HIPAA privacy rule, the result is that there will be more identifiable records maintained as a result of a disclosure that was supposed to be limited to non-identifiable records in the first place.

---

[1] We are using the term *limited data set* as defined by the HIPAA Privacy Rule. As defined by HIPAA, a limited data set is Protected Health Information that excludes certain direct identifiers such as name, street address, telephone number, biometric identifiers (including photographs), and other information. Limited data sets are considered Protected Health Information under HIPAA because the data can still be re-identified in some circumstances. Limited data sets, under current regulation, may only be disclosed for research, public health, or health care operations, and must be released only subject to a formal Data Use Agreement that complies with HIPAA limited data set data use agreement standards. For more, see CFR § 164.514(e), <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf>.

[2] "Because PHI in limited data set form is not completely de-identified, the risk of re-identification is a consideration in determining whether it should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification... ." p. 74 Fed. Reg. 19009.

Inquiries by an individual who has been notified of a breach will create even more identifiable records somewhere. If a limited data set user obtained limited data set records from multiple sources, the confusion will be compounded. Imagine the reaction of a data subject whose records were obtained by a limited data set user from more than one source. Few patients would understand why his or her records were collected from multiple sources, and the individual receiving two (or more) notices about a single breach could be overwhelmed.

Although no solution is going to be perfect regarding limited data sets, we have several proposals.

A. Notification should be required only when re-identification has occurred or is there is a significant likelihood re-identification will occur.

Any significant harm to an individual because of a breach of a limited data set will occur as a result of re-identification. Therefore, we see a potential way to balance the interests here by notifying individuals only when a breach of a limited data set has resulted in re-identification or if there is a significant likelihood that re-identification has, will, or may occur. This standard would be inappropriate for identifiable data, where disclosure to any recipient affects the privacy interest of the data subject. But the standard for limited data set breaches can potentially allow for fewer individual notices in some circumstances because the records are not overly identifiable. (See heading E for our suggestions on expanded non-individual notification of breach to HHS and the public.)

The assessment of likelihood for re-identification is crucial here, and would be based on the amount of data lost (both limited data set and other data that may have been lost with it), the currency of the data, any degree of encryption or coding, and other factors.

We acknowledge that many casual recipients of a laptop with a limited data set would have neither the incentive nor the capability of re-identifying the records. Policy should not be made on the sole assumption that all lost data will end up in the hands of an individual or entity with the skills, equipment, information, and expertise necessary to re-identify data. But neither should policy be made on the sole assumption that no one at any time will have the interest or the means to re-identify the data found in a limited data set. As time goes on and technology improves, re-identification of limited data sets may become child's play.

After a breach, the limited data set user should be required to consult regularly with the covered entity that provided the data to assess whether any evidence on re-identification appears following the breach. Because the limited data set user will not know the identities of the users, it will not be able to evaluate on its own all of the available evidence without assistance. Consultation can be required for a reasonable period of time following the breach, perhaps up to a year.

B. Any organization that has had a breach of limited data sets must proactively disclose the fact of the breach to any covered entity from which it seeks limited data sets for the next five years.

Any covered entity considering disclosure of a limited data set for lawful purposes should know the track record of the proposed recipient. There should be an express regulatory requirement that an entity requesting limited data sets must respond to the question regarding past breaches truthfully covering the preceding five years. If the consequence of a breach is denial of access to limited data set in the future, the result may be a mechanism that will provide limited data set users an additional incentive for careful behavior.

C. Any organization that has had three breach incidents involving limited data sets should be barred from receiving limited data sets for a period of time.

If a user of limited data sets experiences repeated breaches, we propose that the user should be barred from requesting or receiving limited data sets for the next five years. The bar should remain as long as there have been three breaches in the preceding five years.

D. Limited data sets, if they are to be re-identified, should be re-identified with strict controls.

If records must be re-identified, the re-identified records should be segregated and used only for the breach notice and follow up, preferably without disclosure of identifiers to the limited data set user if possible. If notification or re-identification tasks are outsourced to a third party, there must be a data use agreement that specifies the rules for maintenance, use, disclosure, storage, and destruction of the records. All re-identification, notification, and other breach costs must be paid by the limited data set user. These obligations must be part of the original data use agreement with the covered entity that released the limited data set.

E. Increased reporting of limited data set breaches to HHS, covered entities, and the public

We see this rulemaking as an opportunity for HHS to further regulate limited data sets in a way that could result in an overall improvement of the handling of this kind of data. Recipients of limited data sets are already required to report any unauthorized disclosures of the limited data sets to the covered entity with which the recipient has a data use agreement.[3] If limited data sets are not included in individual breach notice, then further "mass" or "public" reporting of breaches involving limited data sets is an important step to add, particularly in a digital environment.

[3] CFR § 164.514(e)(4)(ii)(C)(3).

Whether or not individual breach notices are required, **all limited data set breaches should be reported to HHS by both the covered entity and the limited data set user. The data should be posted on an HHS web site and made available to the public.**

We think that requiring broader reporting of breaches of limited data sets to not just covered entities, but also to HHS and the public could have a positive impact on privacy and consumer trust if done correctly. We also think that a requirement to more robustly and publicly report breaches of limited data sets to covered entities, HHS, and the public could potentially assist covered entities in their compliance regimes.

II. Comments Regarding a Listing of Off-the-Shelf Products

We recommend that HHS not include a listing of "HHS-compliant" off-the-shelf products that meet the encryption standards in its future guidance. HHS should be a neutral arbiter that issues guidelines; HHS is not a product-testing entity. We are concerned about several issues.

First, determining whether a particular product meets the HHS encryption guidance standards would involve a good deal of effort, expertise, and time. Products would have to be reviewed and tested by individuals who could attest to the product quality. The product manufacturers would need to open up their source code for review, and HHS would need to review that code for compliance with the standards.

This kind of review would be required to do even a minimal job of making a determination of compliance, and it would constitute a major undertaking. Even if HHS outsourced the review duties, these tasks could easily overwhelm the Department as multiple vendors sought approval for their products on the HHS list. Without a quality review of the products, inclusion on the HHS list would be reliant on the vendors' assertions of compliance, and HHS would put itself in the position of being a de facto advocate of certain products without having tested those products.

Second, these kinds of technologies change and advance rapidly. If the HHS guidance did not update as rapidly as the products changed, covered entities could be relying on old or outdated products.

For these reasons, we think it would be wise to exclude a listing of specific products in formal HHS guidance. If HHS does decide to go ahead with a specific listing of products, we recommend the following:

1. A full-time staff and adequate budget be allocated to such an effort.
2. Product listings, if they were to be included, should undergo a complete review at least once a year for currency even if the products have not been updated.
3. The review of products should be controlled by HHS and/or NIST, and should not be outsourced as that could potentially introduce conflicts of interest among vendors.

4. HHS should to set up a formal mechanism to accept complaints by users regarding the products on the HHS list. Complaints should be affirmatively disclosed to covered entities that may rely on the listed products and the complaints should be available otherwise to the public.

*****

Thank you for the opportunity to comment. If you have any questions, please contact us.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org
+1 760-436-2489