



230 E. Ohio Street, Suite 500  
Chicago, IL 60611-3269

Tel 312 664 4467  
Fax 312 664 6143

[www.himss.org](http://www.himss.org)

May 21, 2009

The Honorable Kathleen Sebelius  
Secretary of Health and Human Services  
U.S. Department of Health and Human Services  
200 Independence Avenue, SW  
Washington, DC 20201

Dear Secretary Sebelius:

On behalf of the Board of Directors and members of the Healthcare Information and Management Systems Society (HIMSS), I am pleased to submit written comments on the Department of Health and Human Services request for information, entitled, *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009 ( 45 CFR Parts 160 and 164)*, that was posted on the Department's website on April 17, 2009.

HIMSS is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of healthcare. HIMSS represents more than 22,000 individual, 350 corporate members, and 46 chapters nationwide. HIMSS seeks to shape healthcare public policy and industry practices through its educational, professional development, and advocacy initiatives designed to promote information and management systems' contribution to quality patient care.

As in past responses to HHS, HIMSS has leveraged the subject matter expertise of our members to ensure that our response reflects the broadest level of industry experience. For the response on the guidance document, our Privacy and Security Steering Committee played an important role in encouraging comments from their industry colleagues. These cross-industry viewpoints ensure that HIMSS fulfills its requirement to offer a coordinated voice to the national discussion on these important healthcare issues.

With respect to the questions spelled out in Section III. Solicitation of Comments, HIMSS has followed the government's suggestion of dividing the comments into two categories:

- A. Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

***Government Question #1: Are there particular electronic media configurations that may render PHI unusable, unreadable, or indecipherable to unauthorized individuals, such as a fingerprint protected Universal Serial Bus (USB) drive, which are not sufficiently covered by the above and to which guidance should be specifically addressed?***

HIMSS input: HIMSS encourages HHS to conduct/acquire/reference a market survey to uncover available products in this area, such as the one mentioned in the question.

***Government Question #2: With respect to paper PHI, are there additional methods the Department should consider for rendering the information unusable, unreadable, or indecipherable to unauthorized individuals?***

HIMSS input: HIMSS recommends that HHS rely upon NIST Special Publication 800-88 guidance (solely), which calls for cross-cut shredding to 1x5 mm or shredding to no more than 5 mm per side or 25 mm square. The size of the shredded material should be proportionate to the confidentiality and risk. Further, NIST 800-88 guidance states that a key decision on sanitization is whether the media are planned for reuse or recycle. Covered entities and business associates may retain contractual control of the shredded media, which safeguard the confidentiality of the shredded print material by the shred vendor.

***Government Question #3: Are there other methods generally the Department should consider for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals?***

HIMSS input: HHS should rely upon NIST Special Publications 800-52, 800-77, 800-88, 800-111, 800-113 for rendering ePHI unusable, unreadable or indecipherable. Any products or methods that meet these standards should be considered.

***Government Question #4: Are there circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals?***

HIMSS input: HIMSS appreciates the question to the healthcare community. The question is outside the scope of HIMSS member comments.

***Government Question #5: Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals? Can risk of re-identification be alleviated such that the creation of a limited data set could be added to this guidance?***

HIMSS input: HHS included the limited data set in response to comments on the proposed HIPAA regulations that the de-identification standard would curtail important research, public health, and healthcare operations activities. The general intent of creating the limited data set appears to have been to facilitate such activities. Thus, requiring breach notification for the limited data set, when most limited data sets include minimal information, would effectively increase the burden on these activities thereby contradicting the intent of the regulations which was to facilitate such activities.

***Government Question #6: In the event of a breach of protected health information in limited data set form, are there any administrative or legal concerns about the ability to comply with the breach notification requirements?***

HIMSS input: HIMSS recommends including limited data sets in the breach notification requirements would significantly increase the administrative burden on covered entities. A covered entity likely would need to: (1) amend current data use agreement templates to require breach notification; (2) possibly re-execute data use agreements between the covered entity and various researchers; (3) create a process for re-identifying information quickly to meet the notice requirements; (4) in the event of a breach, investigate data that would not be easily re-identified; and (5) significantly expand the scope of information for which a covered entity must meet breach notification requirements. Legal/compliance concerns could arise when data could not be accurately re-identified or re-identified quickly enough to meet the timelines in the rule.

***Government Question #7: Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?***

HIMSS input: HIMSS recommends that HHS rely upon NIST Special Publications 800-52, 800-77, 800-88, 800-111, 800-113 for rendering ePHI unusable, unreadable or indecipherable. While there may be perceived value from specifying in the regulation specific, named off-the-shelf products that should meet the encryption standards, HIMSS believes that this should not be done because information technology products and developments in the off-the-shelf markets move quickly, making such specification practically difficult at best.

This issue could be handled via the product certification process (using Certification Commission for Healthcare Information Technology (CCHIT) or other certification bodies) using criteria specified by NIST. As these criteria are specified yearly, this could address the change in the markets. All new technologies and methodologies that meet the standards should be accepted.

B. Questions on Breach Notification Provisions Generally:

***Government Question #1: Based on experience in complying with state breach notification laws, are there any potential areas of conflict or other issues the Department should consider in promulgating the federal breach notification requirements?***

HIMSS input: HIMSS appreciates the question and would like to highlight comments made by one member on how the issue may apply to cross-border legal considerations as well:

“We have discussed as a topic in the work of the “Southeast Michigan Healthcare Information Exchange” (SEM/HIE) Sub WG for Security & Privacy as I am Chair, the breach notification requirement as part of our “policy agreement” work which is focused on the business level. (We can discuss why that level another time.)

Breach notification came up as a topic because many of the healthcare providers in SE Michigan have operations across the River in Canada and part of our compliance methodology is to deal with “international law”. While this is “US Law”, it might be useful for some guidance to be provided as to how to handle that? There are other States that border Canada, such as Washington State and Mexico, such as Texas or California, so this might come up?

Our policy work is to more automate compliance with “policy” of compliance and Laws and one challenge is that the “Laws” are found in a “paper” environment and I have noted to the group and to the State of Michigan HIT Officials at a number of hearings in Lansing that the State might look to develop a digital repository of the “paper” laws and allow for interface electronically? It would not be good to develop a set of agreed upon policies, of diverse stakeholders of an HIE at the Business Level, deployed as “code” and then discover that the “policy” is in violation of some State or region of a State, some “months” later.

Breach notification is one of those compliance issues that I think, could be “automated” and the while I don’t think some movement to “harmonize” the dates is necessary, it would be nice if “States” could think about providing a digital repository to interface compliance concerns with differing State Law.”

***Government Question #2: Given current obligations under state breach notification laws, do covered entities or business associates anticipate having to send multiple notices to an individual upon discovery of a single breach? Are there circumstances in which the required federal notice would not also satisfy any notice obligations under the state law?***

HIMSS input: HIMSS appreciates the question to the healthcare community. The question is outside the scope of HIMSS member comments.

***Government Question #3: Considering the methodologies discussed in the guidance, are there any circumstances in which a covered entity or business associate would still be***

*required to notify individuals under state laws of a breach of information that has been rendered secured based on federal requirements?*

HIMSS input: HIMSS appreciates the question to the healthcare community. The question is outside the scope of HIMSS member comments.

**Government Question #4:** The Act's definition of "breach" provides for a variety of exceptions. To what particular types of circumstances do entities anticipate these exceptions applying?

HIMSS input: HIMSS appreciates the comment to the healthcare community. We have attached a short spreadsheet that highlights several member observations that should be helpful to the Department's efforts.

The American Recovery and Reinvestment Act has created many challenges and opportunities that or the federal government and the healthcare community. We appreciate your effort to engage healthcare stakeholders in reviewing the guidance document, and look forward to future dialogue with HHS on this important issue. Our staff points of contact are [Mr. Thomas M. Leary](#), Sr. Director for Federal Affairs, and [Ms. Lisa Gallagher](#), Sr. Director for Privacy and Security.

Sincerely,



H. Stephen Lieber, CAE  
HIMSS President/CEO

cc: Ms. Robinsue Frohboese, Acting Director, HHS Office of Civil Rights  
David Blumenthal, MD, MPP, National Coordinator for Health Information Technology