



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)

June 1, 2009

The Honorable Jon Leibowitz  
Federal Trade Commission  
600 Pennsylvania, Avenue, N.W.  
Washington, D.C. 20580

Dear Chairman Leibowitz;

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 (attached) on the Federal Trade Commission's request for information, entitled, "Health Breach Notification Rulemaking, Project No. R911002."

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 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, members of our Personal Health Records and Privacy and Security Steering Committees played important roles 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 notification to the FTC, the American Recovery and Reinvestment Act creates many challenges and opportunities for 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. [Mary Griskewicz](#), Sr. Director for Ambulatory Information Systems.

Sincerely,

A handwritten signature in black ink that reads "Steve Lieber". The signature is written in a cursive, flowing style.

H. Stephen Lieber, CAE  
HIMSS President/CEO

Attachment: HIMSS Response to FTC Health Breach Notification Project # R911002

cc: David Blumenthal, MD, MPP, National Coordinator for Health Information Technology

**Response to the Federal Trade Commission**



**Health Breach Notification Rulemaking, Project No. R911002  
June 1, 2009**

***Part 318- Health Breach Notification Rule comments***

***318.3 Breach notification requirement.***

HIMSS input

HIMSS recommends that even if the information breached in the PHR was de-identified, it must be reported to the consumer. This will allow for monitoring of potential medical identity theft, as well as any unauthorized usage of PHI.

HIMSS input

Regarding Section II analysis on page 18 of the draft rule: “reasonably should have been known about the breach” standard. The Commission expects entities that collect and store unsecured PHR information to maintain reasonable security measures, including breach detection measures, which should assist them in discovering breaches in a timely manner.” For information to be breached, it must first be in a secure state – specifically, as electronic personal health information. It is impossible to secure information that was not first in a secure state in the PHR.

***318.5 Methods of Notice***

***a. Individual Notice***

HIMSS input

HIMSS recommends that the consumer of the PHR also has a responsibility to keep his/her contact information up-to-date to support. Such responsibility should be noted.

HIMSS input

As the PHR is an electronic tool as outlined in your PHR definition, HIMSS strongly recommends electronic notification to consumers by the PHR vendor company. When a breach occurs, HIMSS recommends that the PHR vendor company must direct breached PHR owners to a notification page. Such direction should occur when the consumer logs-in to the PHR, hence notifying the consumer that his/her information may have been breached.

***c. Notice to the FTC***

HIMSS input

HIMSS agrees that vendors of PHRs and PHR-related entities shall provide notice to the Federal Trade Commission following the discovery of a breach of security. The FTC should not prescribe how the notification should take place, as some remedies could be costly to the PHR vendor or related entity, i.e. media notification. The PHR is an electronic tool and the primary medium for the consumer is electronic.