Oct. 22, 2009

The Hon. Kathleen Sebelius
Secretary
United States Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

**RIN 0991-AB56**
**HITECH Breach Notification for**
**Unsecured Protected Health Information Rulemaking**

Dear Madam Secretary:

I am writing to express our deepest concern about the interim final regulations on Breach Notification for Unsecured Protected Health Information promulgated on Aug. 24, 2009. The Department of Health and Human Services was charged with developing regulations under the American Recovery and Reinvestment Act of 2009 (ARRA) to govern electronic medical records maintained by insurers, health care providers and others covered by HIPPA. The Federal Trade Commission was charged with writing breach rules for Personal Health Record vendors, such as Google, which are not covered by HIPPA.

Among the provisions of ARRA were innovations to promote health information technology as a way to improve quality and efficiency of the nation's health care system. Those improvements can only be realized if there are strong safeguards that protect the privacy and security of individuals' personal health records. Consumers must be able to trust the security of these electronic systems.

Congress recognized this importance in Section 13402 of ARRA when it required notification if there is an "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information." This is a simple, black and white standard. If there is a breach, there must be notification. Such a standard helps build public trust, because if there is ever a problem, consumers know they will be informed. Moreover, ARRA provides a safe harbor for information that is released which has been rendered unusable, unreadable, or indecipherable. Mandatory breach notification with this safe harbor provides a strong incentive for health care entities to protect data through encryption and other means.

Inexplicably, and flouting Congressional intent, the Department of Health and Human Services has introduced a "harm" standard before breach notification is required. You have decided to interpret "compromises the security" of data to include a substantial harm standard. Under the HHS interpretation, if the breaching entity decides there is no significant risk of financial, reputation or other harm to the individual, the provider or health insurer never has to disclose that the sensitive information was used or disclosed in violation of the federal privacy rule.

In other words, the company responsible for protecting the sensitive data gets to decide if it needs to bother to tell anyone that sensitive health data was breached. This is simply outrageous. It is even more troublesome

when one recalls that the House Committee on Energy and Commerce considered a similar "harm" standard during discussions of health and information technology legislation in May 2008. Committee members considered public comments and practices of various states; they explicitly rejected a " harm" standard.

Explaining their reasoning Rep. Henry Waxman, Rep. Charles B. Rangel, Rep. John Dingell, Rep. Frank Pallone Jr., Rep. Pete Fortney Stark and Rep. Joe Barton have written:

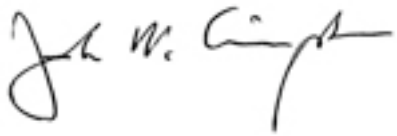
> *"The primary purpose for mandatory breach notification is to provide incentives for health care entities to protect data, such as through strong encryption or destruction methodologies and to allow individuals to assess the level of unauthorized use of disclosure of their information. Such transparency allows the consumer to judge the quality of a health care entity's privacy protection based on how many breaches occur, enabling them to choose entities with better privacy practices. Furthermore, a black and white standard makes implementation and enforcement simpler."*

What prompted the Department to flout Congressional intent remains unclear. Could it be that Congress managed to fend off the pressures of the health care industry in passing ARRA only to have the lobbyists return to exert their influence on the rule making process?

It is interesting to note that the Federal Trade Commission, charged with promulgating breach regulations for non-HIPPA entities such as Personal Health Records vendors did not find any justification for introducing a "harm" standard. The FTC remained true to Congressional intent and to promoting the public interest.

I call upon HHS to repeal the harm standard immediately and fully and properly implement what Congress enacted.

Sincerely,



John M. Simpson
Consumer advocate.