



Michael D. Maves, MD, MBA, Executive Vice President, CEO

May 29, 2009

The Honorable Jon Leibowitz
Chairman
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

RE: Health Breach Notification Rulemaking, Project No. R911002

Dear Chairman Leibowitz:

The Federal Trade Commission's (FTC) proposed rule outlines the breach notification requirements for vendors of personal health records (PHRs) and related entities, including notice timelines, methods, and content for notifying affected individuals and the FTC when the security of individually identifiable health information has been breached.

The FTC's proposed rule acknowledges that under the "American Recovery and Reinvestment Act of 2009" (ARRA: P. L. No. 111-5), the Department of Health and Human Services (HHS) must also promulgate interim final regulations related to breach notification requirements for HIPAA-covered entities and their business associates. The FTC further states that the FTC's proposed rule on breach notification requirements applies to vendors of PHRs, PHR-related entities, and third party service providers, and that it does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. **To avoid confusion regarding the scope of the FTC rule, the American Medical Association (AMA) urges the Commission to clearly indicate in the Final Rule that the FTC's health breach notification requirements do not apply to HIPAA-covered entities (i.e., physicians) and their business associates even if they are involved with PHR products and/or services, use a system that has PHR capabilities, including but not limited to the ability to access information in a PHR or send information to a PHR.**

The Honorable Jon Leibowitz

June 1, 2009

Page 2

The AMA also strongly recommends that the FTC and HHS work closely together to assess the extent to which vendors of PHRs, PHR-related entities, and third party service providers may be HIPAA-covered entities or business associates of HIPAA-covered entities. In addition, the FTC and HHS should ensure that the breach notification requirements are effective but are not overly burdensome or costly to implement and follow. Coordination between FTC and HHS to come up with the requirements is essential in order to avoid circumstances in which consumers may receive multiple, duplicative breach notices over the same incident. Moreover, overly burdensome, costly requirements may act as a disincentive for widespread PHR and electronic health records adoption and use. Finally, both the FTC and HHS should pursue comprehensive outreach and education initiatives so that all affected parties fully understand the requirements and responsibilities.

The AMA appreciates the opportunity to comment. Should you have any questions about our comments, please direct them to Mari Savickis, Assistant Director, Division of Federal Affairs, at mari.savickis@ama-assn.org or 202-789-7414.

Sincerely,

2

Michael D. Maves, MD, MBA