American Insurance Association

2101 L Street NW
Suite 400
Washington, DC 20037
202-828-7100
Fax 202-293-1219
www.aiadc.org

June 1, 2009

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Health Breach Notification Rulemaking, Project No. R911002

The American Insurance Association (AIA) is a trade association which represents property and casualty insurers doing business across the country and around the world. As entities subject to state security breach notification laws, we find it important to comment on the Federal Trade Commission's (FTC) proposed Health Breach Notification Rule. Financial services regulators often look to one another's work product when developing their own guidance or regulations. Consistency in approach to breach notification is crucial.

Consistency with Other Laws and Regulations

AIA encourages the FTC to work with the Department of Health and Human Services (HHS) when finalizing its guidance to ensure that there are no discrepancies that could lead to confusion and increased notification.

AIA also encourages FTC to consider the potential difficulty the differences in state breach notification laws and the FTC guidance creates for entities. Consider a few examples.

- First, Massachusetts prohibits an entity from telling a consumer what elements of personal information were involved in a breach, however the FTC proposed rule requires that the notice contain these elements. (Section 318.6(b))

- Second, most states allow notice to be provided in "the most expedient time possible without unreasonable delay", without setting a specific time limit. The FTC proposed rule requires notification within 60 days. (Section 318.4(a))

- Third, the definition of "breach of security" should clarify that harm is required to trigger notification. Many State breach notification laws require an element of harm. (Section 318.2(a))

These and other differences in state breach notification laws and the FTC proposed rule could result in multiple notices for the same event or notification under the FTC rule but not under well-established state laws. It is important that FTC consider the different state breach notification laws when developing its guidance.

Substantive Concerns with FTC Guidance

AIA members continue to review the FTC proposed rule and to work through the implications of it and of the ARRA. Several of the concerns identified to date center on the document's potentially overbroad scope and others deal with implementation direction.

(1) Harm Trigger
Section 318.2(a)

The definition of "breach of security" should make it clear that the trigger is a reasonable expectation of harm resulting in unauthorized acquisition. The following proposed revision clarifies this point: … Unauthorized acquisition will be presumed not to include unauthorized access to unsecured PHR identifiable health information if ~~unless~~ the vendor… An element of harm ensures that consumers do not become unnecessarily worried. It also prevents a frequency of unnecessary notices which consumers may become apathetic towards. It is important that the FTC consider the harm element when developing its rules, so that breach notification is meaningful.

(2) Scope – Definitions of "Personal Health Record," "PHR related entity" and "Vendor of personal health records"
Sections 318.2(d), 318.2(f), 318.2(i)

The Conference Report of the Recovery Act should guide the drafting of the definition of "personal health record," "PHR related entity" and "vendor of personal health information." It specifically mentions not including "the kinds of records managed by or primarily for commercial enterprises." This same scope clarification should be incorporated into the FTC's definitions.

(3) Substitute Notice
Section 318.5(a)(4)

For those supplying a substitute notice (where there is insufficient contact information for 10 or more individuals) there should be more detail for those seeking to comply. For example, businesses would have more compliance certainty if they knew: (1) what would be deemed adequate in terms of the duration for maintaining the notice; (2) what are acceptable considerations for the purpose of defining major print or broadcast media, which are "reasonably calculated to reach the individuals affected"; and (3) whether the media chosen should be based on where the institution believes the people lived.

Conclusion

AIA urges the FTC to work with HHS as it finalizes it proposed rule, consider the impact the rule has on state breach notification laws, provide additional detail regarding substitute notice, and to clarify that there is an element of harm in the notification trigger. AIA also asks to be permitted to supplement these comments as we work with members to understand the proposed rule as well as other related materials.

Thank you for your consideration of these comments. AIA appreciates the opportunity to comment on the FTC proposed rule and is available to answer any questions.

Respectfully submitted,

/s/

Angela Gleason
Associate Counsel