



1730 M Street, NW, Suite 502  
Washington, DC 20036

phone » (202) 659-9440  
fax » (202) 659-9422  
web » www.ahima.org

May 29, 2009

US 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

Ladies and Gentlemen:

The American Health Information Management Association (AHIMA) welcomes the opportunity to comment on the Federal Trade Commission's (FTC's or Commission's) proposed rulemaking on Health Breach Notification as posted in the April 20, 2009 *Federal Register* (Vol. 74, No.74).

AHIMA is a not-for-profit professional association representing more than 53,000 health information management (HIM) professionals who work throughout the healthcare industry in both HIPAA and non-HIPAA related entities. HIM professionals are educated, trained, and certified to serve the healthcare industry and the public by managing, analyzing, protecting, reporting, releasing, and utilizing data vital for patient care, while making it accessible to patients, healthcare providers and appropriate researchers when it is needed most.

Insuring patient information confidentiality and security has been a significant function of our profession for many decades; and with the introduction of the HIPAA privacy and security requirements, AHIMA established and has maintained considerable attention to these topics as well as establishing a certification for professionals specifically in healthcare privacy and security. With the increase of identity theft in the nation, AHIMA members have turned their attention to this problem and we welcome the Congress, the Department of Health and Human Services (HHS) and the FTC's work with regard to this issue as well. The HIM profession believes that addressing confidentiality and security is key to maintaining consumers' trust. AHIMA has been an advocate for the use of personal health records (PHRs) for many years<sup>1</sup> and also an advocate for the conversion of the healthcare industry to electronic health records (EHRs) and electronic health information exchange (HIE). We believe that the development and use of these tools can only occur when there is consumer trust, and we welcome and support the FTC's efforts in this regard.

---

<sup>1</sup> In fact, AHIMA has maintained a website dedicated to promoting consumer understanding and interest in the use of PHRs – [www.myPHR.com](http://www.myPHR.com).

In consultation with our members and expert staff we have the following comments related to your proposed rulemaking. Our comments follow your section-by-section analysis and statement of the proposed rule.

### **Proposed Section 318.1 – Purpose and Scope:**

It must be noted that AHIMA believes that protected health information (PHI) or identifiable health information must receive the protection of law no matter who acquires, accesses, or uses the data. Currently, neither the Health Insurance Portability and Accountability Act of 1996 (HIPAA) nor the American Recovery and Reinvestment Act of 2009 (ARRA) fully cover all entities that may legitimately hold such health information, and it is unclear with the current hodgepodge of state laws whether all health data is actually protected. ARRA requires the FTC to cover PHR identifiable health information and we believe that it provides a good step toward the protection of individual's health information; it just is not complete in all situations.

The FTC raises several questions related to scope, which we have found difficult to answer due to the changing nature of PHRs and those who offer or support such products.

PHRs come in a variety of offerings from providers, health plans, and HIPAA-related covered entities. But there are also PHRs offered by various Internet-related companies, such as Google and Microsoft, as well as health record banks. Some PHRs are also “sponsored” by third parties including employers, unions, and other social groups who do not have status under HIPAA. There are relationships between these non-HIPAA related organizations and HIPAA covered entities that will require close scrutiny to determine whether they are or are not HIPAA-related especially given the expansion of HIPAA applications to what were previously known as “business associates.” ARRA also has extended the “business associate” definition to entities such as HIE organizations. With these products and relationships in flux, we believe that the regulations of both the FTC and HHS will have to be written to allow revision as the PHR-related products and the relationship between PHR operators and HIPAA covered entities mature. We do not see this stabilizing in the next few years.

As noted, the ARRA provisions exclude HIPAA-related covered entities from the FTC's jurisdiction, however, HIPAA allows some organizations to segregate their HIPAA entity from the rest of the organization. So, the possibility exists that a large enterprise could have among its entities a HIPAA-related entity, or a HIPAA “business associate” entity, and a separate entity that offers, operates, or supports PHRs. There is also the potential for a HIPAA “covered entity,” such as a clearinghouse, to offer HIPAA related services to HIPAA entities, but in a separate line of products offer PHRs to consumers, with no connections between the two. Probably there would not be a situation where a breach would impact both of these sub-corporate entities, but the potential is there. Could an individual then receive more than one breach notification? Yes, but we believe the potential is quite small and given the circumstance, appropriate. Certainly, in any of these mixed situations, the entity involved will need to provide proof that a breach was limited to one and not all of the other potential entities. (See comments on state law below.)

### **Proposed Section 318.2 – Definitions:**

- a) **Breach of security** – we appreciate the discussion regarding this definition and agree with the Commission’s definition.
- b) **Business associate** – we agree with this definition.
- c) **HIPAA-covered entity** – we agree with this definition
- d) **Personal health record** – we agree that this definition follows that provided in ARRA, however, we also note that the definition expands beyond some of the definitions currently used and may be confusing to consumers. Consumers will need to be educated on just what type of records can be considered PHRs under this rule.
- e) **PHR identifiable health information** – we agree with the definition since it references the HHS definition. We note that this definition could be changed by HHS in the future and therefore this definition should continue to be consistent with the HHS definition in the future.
- f) **PHR related entity** – we agree with the definition, however, we are concerned that f-1 and f-2 refer to use of websites and do not recognize the potential for such products or services to be offered through printed means via a vendor of personal health records or via a HIPAA-related provider.
- g) **Third party service provider** – we agree with this definition.
- h) **Unsecured** – the reference to the secondary definition (that which would be used if the HHS Secretary had not promulgated a definition) appears unnecessary. What is needed, however, is a reference to the current specified guidance of the HHS Secretary to recognize that this definition could change over time and users of the technology will be responsible to upgrade their security compliance in order to prove that data is secured.
- i) **Vendor of personal health records** – the definition appears adequate, but we must note our comments above related to your questions under 318.1.

As noted above, there is a unique situation with PHRs where a third party might sponsor a PHR. For instance an employer might sponsor a PHR which is operated by a private vendor. Clearly the vendor would be the site of the breach; however, the sponsor might also have some obligation if Protected Health Information PHI flows through such a sponsor to the PHR. While this may be already within the definitions presented, AHIMA members believe it would be clearer to include the sponsors specifically in the rule and these definitions.

### **Proposed Section 318.3 – Breach Notification Requirement:**

AHIMA welcomes the Commission’s additional language in 418.3 (b) related to “...provide notice of the breach to a senior official at the vendor...” This is an excellent step and if possible, we believe this concept ought to be extended to any agreement or contract between these parties so that a specific senior official and alternate senior official are identified specifically by role.

This section also raises the question as to whether the various parties – PHR related entity, third party service provider, or vendor of personal health records – ought to be required to have a contract or agreement that reflects the requirements of these sections similar to the “business associate agreement (BAA)” under HIPAA. A HIPAA-covered entity offering a similar PHR product would be required to have a BAA.

We are in agreement with the remainder of this section.

#### **Proposed Section 318.4 – Timeliness of notification:**

AHIMA is in agreement with this proposed section, and agrees with the language added regarding “without unreasonable delay.”

[It should be noted that a review of the state breach notification laws/regulations revealed only two states that mandated specific time periods for breach notification at this time. California Health and Safety Code section 1280.15 requires that individuals affected by the breach receive notification within 5 days following discovery. Florida State Ann. 817.5681 et seq. which requires that notification must be made no later than 45 day following determination of the breach. West Virginia, WV Code 46A-2A-101 et seq., effective June 26, 2008 requires that the breach notification be sent as soon as practicable following discovery of the breach. The District of Columbia, DC Code Sec 28-3851 et seq., effective January 1, 2008 requires that the entity shall promptly notify any District of Columbia resident whose personal information was included in a breach. A review of state breach notification laws/regulations of 32 states did not reveal a requirement of a mandated specific time period for breach notification; instead these states chose to use the less stringent wording, “in the most expeditious time/manner possible without unreasonable delay.”]

#### **Proposed Section 318.5 – Methods of notice:**

AHIMA agrees with the Commission’s concerns regarding consumer consent (a) (1) as expressed in footnote 16 on page 74FR17918; however, we do not see this concern transferred to the actual requirements under this section. We suggest that the concern be made into an explicit requirement for consumers to have an explicit agreement for the notification by e-mail.

AHIMA likewise agrees with the Commission’s concerns for the posting of a notice of breach (a) (4) (A) on the entity’s webpage; however, once again, the Commission’s recommendations on how to make the notice more conspicuous to, and understood by, consumers does not translate into the regulation as proposed.

AHIMA’s members are especially concerned that the FTC must be notified within 5 days of any breach discovered affecting 500 or more individuals. The concern is that 5 days may not be sufficient to determine if there is an actual breach including some of the investigation activities discussed by the Commission in presenting the regulation. We recognize the FTC’s need to know and support prompt notification of the individuals involved, but it is unclear just what steps the FTC might take at this

point, and what might happen if any action is taken by the FTC before the entity's investigation is complete. We understand the concern to have a short window between discovery and notification of individuals, but we are also concerned that consumers could be needlessly affected by an announcement that turns out to be a false alarm. Perhaps some clarification of the steps the FTC might take at the point of the 5-day notice would negate the concerns that were raised.

The proposed rule states that if 10 or more individuals cannot be reached, the vendor of personal health records or PHR related entity must provide notice in one of two forms: 1) home page of its website, 2.) notice in major print or broadcast media. Concerns were raised about the reporting threshold variations that exist between the FTC proposed rule and the existing state breach notification laws/regulations. A review of the state laws revealed stark variation in the established breach notification threshold triggers for determining the appropriate method of notice. It was noted that the state laws would often employ monetary expense and affected population metrics that are out of alignment with the FTC recommended trigger thresholds. A review of 35 identified state breach notification laws/regulations revealed a range of reporting threshold variations between notification costs exceeding \$5,000 and affected populations exceeding 1,000 residents and notification costs exceeding \$250,000 and affected populations exceeding 500,000 residents. Seventeen states set their substitute notice threshold levels at notification costs exceeding \$250,000 and affected populations exceeding 500,000 residents.

#### **Proposed Section 318.6 – Content of notice:**

Once again, our comments on this section relate to the discussion the Commission has on its rationale for the proposed section versus the final language proposed in this section. We agree with the Commission's concerns and wish to see them more explicit in the actual regulation. AHIMA plans to work with its members to develop model language that could be used in these situations and we appreciate the Commission's expertise in this and other sections.

#### **Other Proposed Sections:**

AHIMA notes that the additional sections (318.7, 318.8, and 318.9) reflect the language of ARRA, and no further comment is needed.

#### **Other Comments:**

##### *State laws*

One issue not addressed in the proposed sections and the background of the Commission's proposed requirements is the impact of state laws and regulations that may overlap these proposed requirements. It has been the experience of AHIMA members that overlapping and often conflicting laws and regulation generally lead to confusion both on the part of the covered entity as well as the consumer. This confusion grows even greater when a federal regulation, such as those proposed here by the FTC, overlaps with several states that may be served by an entity. With the potential for electronic PHRs to be operated by a vendor across several states, this problem explodes. AHIMA recommends that the FTC be cognizant and work with states to eliminate the lack of conformity and overlapping requirements that could lead to avoidance of breach notification, multiple jurisdictions involved simultaneously, or confusion and worry for consumers. While AHIMA members support fully the

need for privacy and security, this overlap and confusion could result in either limited consumer involvement, or limited PHRs being offered.

*The changing environment of PHRs*

We recognize that ARRA provides for an on-going monitoring of the breach notification processes as well as the problem of breaches themselves. As noted above, the environment surrounding PHRs is changing, with regard to products, standards, and use by consumers and others in the healthcare system. We urge the FTC (as we have and will urge HHS) to work with the industry and professionals such as ourselves to ensure that these regulations continue to reflect and appropriately meet the need for confidentiality, privacy, and security as the healthcare system and information technologies continue to change. AHIMA welcomes the opportunity to provide any information and expertise to such an endeavor. As noted, AHIMA has undertaken an effort to identify both federal and state laws and regulations related to breaches of PHI and we would be pleased to share this information. Likewise, AHIMA looks forward to working with the FTC to ensure that the education needed by covered entities and consumers reflect the letter of the law and best practices now and in the future.

**Conclusion**

AHIMA appreciates the opportunity to comment on the proposed rule as published by the FTC. AHIMA is very concerned with providing adequate security and confidentiality protections to all healthcare data no matter where it resides, and the Association has a history of working with our members, the federal government, and the healthcare industry to ensure that these protections and other practices are actively in place.

We realize the Commission has been given a short time to meet certain obligations related to breach notification under the ARRA, and if there is anything AHIMA can do to assist, please contact us. If there are any questions related to the comments in this letter or AHIMA's activities related to confidentiality and security, please contact me at the phone number above or at [dan.rode@ahima.org](mailto:dan.rode@ahima.org). In my absence please feel free to contact AHIMA's director for federal affairs, Allison Viola, at the same phone number or [allison.viola@ahima.org](mailto:allison.viola@ahima.org). Thank you for your consideration and attention and your support of the healthcare industry.

Sincerely,



Dan Rode, MBA, CHPS, FHFMA  
Vice President, Policy and Government Relations

cc. Allison Viola, MBA, RHIA