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

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

AHIMA
American Health Information Management Association®

October 21, 2009

Georgia Verdugo
Office for Civil Rights
US Department of Health and Human Services
Attention: HITECH Breach Notification
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

RE: RIN 0-AB56:
Breach Notification for Unsecured Protected Health Information

Dear Ms. Verdugo:

The American Health Information Management Association (AHIMA) welcomes the opportunity to comment on the Office for Civil Rights (OCR) interim final rulemaking (IFR) on "Breach Notification for Unsecured Protected Health Information" as posted in the August 24, 2009 *Federal Register* (Vol. 74, No.162).

AHIMA is a not-for-profit professional association representing more than 54,000 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 the HIM profession for decades. With the introduction of the HIPAA privacy and security requirements, AHIMA focused considerable attention and education on these topics and established a certification for HIM professionals specifically in healthcare privacy and security.

With the increase of incidents of breach of health information and medical identity theft across the nation, AHIMA members have turned their attention to addressing this problem and welcome the Congress, the Department of Health and Human Services (HHS), and the FTC's attention and work with regard to this issue. The HIM profession believes that addressing confidentiality and security is crucial to maintaining consumers' trust in our healthcare systems. AHIMA has been an advocate for the conversion of the healthcare industry to electronic health records (EHRs) and electronic health information exchange (HIE) as well as the use of personal

health records (PHRs) for many years.[1] We believe that the development and use of these HIT tools can only occur when there is consumer trust, and we welcome and support ONC's efforts in this regard.

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.

Guidance Specifying the Technologies and Methodologies …Individuals [74FR42741-43]

AHIMA agrees with the guidance specified by OCR at this time. We also appreciate that this guidance will change with time and technology and we look forward to participating in the discussions that lead up to future guidance being issued, and hope that the Office will consider providing such opportunities on a regular basis.

AHIMA also appreciates the manner in which the new requirements have been folded into the previous HIPAA rules. Not only does this facilitate coordinating the breach processes with the HIPAA Rule as required, but also serves as a means of highlighting the previous HIPAA requirements as facilities undergo new training related to breach notification. Likewise, we appreciate the work that has been accomplished with the Federal Trade Commission (FTC) to ensure compatibility, for the most part between the two sets of requirements.

Section-by-Section Description of Interim Final Rule [74FR42743-57]

[To shorten our comments and your reading, we will only highlight sections where there is a need to relate a specific positive or negative concern. **No comment signifies our support of the proposed language and intent.** AHIMA appreciates the detail OCR provided in the preamble to this IFR.]

B. Definitions – Section 164.402 – 1. Breach – "Harm Threshold" and "Risk Assessment" [74FR42743-42746]

Under the discussion of "Compromise the Security or Privacy of Protected Health Information," the NPRM discusses the concept of a "Harm Threshold." You also discuss the process for "risk assessment," with regard to determining the harm threshold. This is an issue of high concern for HIM professionals acting in the capacity of a privacy or security officer, and we appreciate the depth of the discussion offered by OCR in regard to this matter.

The HIM profession also deems a considerable obligation to individuals who are the subject of the health information and data for which HIM is a custodian. We recognize the potential harm that can befall an individual and the fact that this harm varies with regard to the data or information involved,; the individual (subject of the data); the facility, practice, or other entity holding the information and subject to the breach; and a variety of environmental factors that

[1] In fact, AHIMA has maintained a website dedicated to promoting consumer understanding and interest in the use of PHRs – www.myPHR.com.

involve the individual's family, community, employment and so forth. We also recognize the disparity between the approach that OCR is suggesting and that taken by the FTC whose subject entities do not necessarily have the environment created by HIPAA and the healthcare industries other protocols as do HIPAA-related entities.

The easiest approach from a cost and decision making perspective would be providing breach notification in all cases without a harm threshold. However, this approach has a number of significant negatives that do not support such an approach including the potential for:

- Organizations to ignore the need to conduct a thorough risk assessment not only to determine if a breach or possible breach occurred, but also the information and changes necessary to incorporate to prevent further occurrences of whatever problems or situations arise.
- Individuals to receive many occurrences of breach notifications from multiple sources, to the point where such notices are ignored because they become insignificant due to volume. This in turn can lead to an ongoing individual and communal distrust of health information systems in general or an ignoring of a situation that calls for action on the part of the individual to reduce further harm.

With the discussion OCR presented and based on our own discussions we agree that a harm threshold is appropriate and necessary. We have a number of suggestions that we believe should be incorporated into the rule and OCR's education activities to make the use of a harm threshold appropriate[2]:

- OCR should consider all comments to the IFR and incorporate concerns related to harm either into a set of criteria which covered entities must consider in determining harm and/or build such considerations (that should be undertaken in a risk assessment) into education programs for covered entities and the healthcare community in general. For instance, "harm" must be considered as described in the IFR but also on the basis of:
  - Type of entity or service
  - The individual's diagnosis or presenting symptoms
  - The type and size of the community in which the services were rendered or the individual resides – it was noted that in a small community harm can come in the form of gossip and other forms of harm to an individual or family's reputation, etc.
  - The type of information – for example a full record versus a collection of orders, reports, etc., and the form of identity on the orders, reports and so forth
  - The potential that family members beyond the individual, personal representative, or designated guardian could have access to the information due to their role in the workforce of the covered entity or employment in the business associate, if known
  - The information involved being part of a "PHR" data base, which by ARRA definition is controlled by the individual and therefore requires the individual to release all information. [Patient portals may not be considered "PHR," but this will depend on how such a record is defined by the organization.]
- If a covered entity through its investigation and risk assessment determines a breach was intentional to gain access to an individual or group's health information, then the individual(s) must be notified.
- When an investigation results in any doubt as to harm, the entity must notify the individual(s) as specified in the Rule.

[2] AHIMA will also be incorporating these recommendations into our own training and education efforts.

- OCR should consider further requirements in the rule that mandate not only that covered entities must undertake a timely risk assessment in all cases, but also document the conduct and results of the risk assessment even if the episode does not result in a finding of breach and any reporting of such a breach. This already is essentially a requirement in several states.

  It has been suggested that entities might hide behind a harm threshold, to take less than adequate approach to risk assessments, however in our conversations we have discovered a high percentage of organizations that suggest that their legal counsel is taking a conservative approach to the breach requirements and recommending organizations notify individuals in all cases, which leads us to the concerns addressed above including a concern that a complete risk assessment might be waived in favor of the breach notification.

  Beyond the concern previously addressed, we also ask that the OCR clarify whether, in situations where more than one individual is involved in a breach situation, an entity must determine the harm to each and every individual and handle each appropriately, or assume that if there is potential harm to one individual, then there is potential harm to all and proceed with a breach notification to all.

C. Notification to Individuals – Section 164.404 – Breaches Treated as Discovered [74FR42749]

Discovery is determined by someone knowledgeable as to what might constitute a breach. This calls therefore for a knowledgeable workforce and business associates. While the HIPAA Privacy Rule §165.530 (b) (2) (C) covers the need to retrain a workforce when material change becomes effective , we believe this needs to be reemphasized in the OCR's publications to the industry by declaring these new rules as a "material change" to the HIPAA Rule. In addition to this added workforce individual responsibility, the OCR and affected entities should also make workforce individuals (other than volunteers) responsible to mitigate the situation if possible. Finally, as stated in the HIPAA Privacy Rule, entity policies and procedures should be brought up to date by the compliance date identified by the OCR.

F. Notification by a Business Associate – Section 164.410 [74FR42753-55]

We understand your discussion on notification by a business associate, and the differentiation regarding business associates who are agents and those who are not; however, we find that this differentiation is confusing to many covered entities whom we have encountered, as well as to consumers who do not understand your timeliness discussion on page 74FR42749, which argues that 60 days should be an outer limit on delaying a notification, and the discussion on page 74FR42754 which then essentially permits a 120-day outer limit in situations where the business associate is not an agent of the covered entity. While this "extension" issue could be addressed through contractual language between the entity and the business associate, it is often the business associate that holds the upper hand in determining what language will be in such a contract. While your language recognizes this, consumers may not.

AHIMA members view breaches as very serious, and recognize the harm to individuals and to the trust of individuals in the entity and in electronic health information systems as well. Delays in notification when a harmful breach has occurred can only serve to erode the trust

consumers have in healthcare entities and the system of electronic health records and interchange we are trying to implement. We urge OCR to consider some means by which non-agent business associates can be made to respond similarly to agent business associates – either in these regulations, or in future regulations surrounding the HITECH law with regard to business associates.

When considering time lines for business associates, we also suggest that business associates be given a short period in which to contact the HIPAA-covered entity of the situation. Many business associates have no contact with the individual whose information may be the subject of the breach, and while covered-entities might be able to provide for earlier contact though a renegotiated contract or business associate agreement, in many cases the business associate has the upper hand – some larger banks, vendors, and services agencies, for example – where the covered entity cannot extract an earlier contact and has limited alternatives for seeking another business associate. The basic relationship is between the individual and the covered entity and if the covered entity does not have the proper time to do its own risk assessment and take other necessary actions, the whole process of breach notification may have more negative results than positive. Loss of faith in covered entities could have a negative effect on the provision of healthcare, something that should be avoided as much as the elimination of breaches themselves.

J. Preemption [74FR42756]

Once again, covered entities and business associates find themselves caught between state and federal regulations. Fortunately, from our conversations we find that most state requirements are stricter than the federal requirements as the IFR points out. However, it is the discrepancy between federal and state requirements that we believe could cause harm to individuals and the national goal for electronic health information as we have pointed out elsewhere. Accordingly, we recommend that once the compliance dates are reached for this IFR, HHS, in concert with Congress and the states, take steps to work with the states to harmonize these requirements and the other HIPAA privacy and security requirements, so that consumers and healthcare providers and plans have one uniform set of requirements rather than the continual need to determine the conflicts that exist in statute and regulations, that lead to a more costly healthcare system and often lead to unintentional errors in following the various requirements.

K. Effective/Compliance Date [74FR42756-57]

We welcome OCR's recognition of the transformation difficulties that exist with this IFR and the dates imposed by the HITECH legislation. However, in providing the February 22, 2010, compliance date, some confusion has been brought to our attention that should be addressed by the OCR. The discussion on compliance notes that the OCR will use its enforcement discretion to not impose sanctions for failure to provide the required notification for breaches during the interim period until February. This does not eliminate the obligations of the covered entities. We have received a number of questions that call for further clarification of the Office, including:

- Will a HIPAA-related entity be out of compliance with regard to changes in the Privacy section of HIPAA, Subpart E, if the training of the workforce is not completed until sometime between the effective date and the compliance date?

- Are we correct in assuming that the OCR anticipates that all covered entities will conduct new training for its workforce in these training sessions?
- Must a HIPAA-related entity report breaches (logged) to the Secretary, as now required as of September 23, 2009, even if it did not issue a breach notification to the individual, media, or Secretary as required?

V. Impact Statement and Other Required Analyses [74FR42757-66]

At this point we have not developed detailed comments on this section, since OCR collected most of these comments in September. In reviewing the processes detailed by OCR and working with our members we have, however, arrived at the conclusion that the amount of effort and cost at implementing these requirements will be significantly higher than that estimated by OCR in this IFR. We are finding the numbers of business associate agreements to be in excess of 70 for many hospitals due to the conservative approach many have taken in order to be in full compliance with the HIPAA privacy and security rules. We are also seeing these requirements creating a new product, for insurance coverage for the costs of breach risk assessment and notification on the part of both business associates and covered entities.

As stated above, we understand and accept the need to address breaches in health information confidentiality and security, and this need supersedes the cost of compliance and hopefully will result in greater compliance with the requirements for confidentiality, privacy, and security. But, this cost also requires that HHS, OCR, and the Office of the National Coordinator for HIT (ONC) work with the industry as further regulations are developed under HITECH to ensure that the package of requirements is harmonized to maximize protections while keeping the costs of transformation and compliance as low as possible.

While the relationship between covered entities and business associates is not the focus of this breach notification IFR, per se, we do believe that HHS and OCR should revisit the requirements for business associate agreements at some point, to determine if the actual agreements and the costs and resources incurred meet the intent of the original rules and whether the rules need to be revised accordingly.

Conclusion

AHIMA's comments are meant to provide better compliance with the HITECH legislation and the need to secure health information in order to eliminate information breaches, but when a breach does occur, provide for both protection for the individuals whose data has been breached and corrective action to be taken to prevent future breaches of the same or similar type that occurred. As the IFR preamble explained, there are several situations created by the inclusion of the new HITECH related rules with the HIPAA rules concerning privacy and security that call for responsible, conscientious action (including risk assessment) and decision making by HIPAA-covered entities and business associates with the patient/individual protections in mind and focus.

Clear regulations can assist in this goal being reached along with quick response in the form of FAQ that ONC has used well in the past. Education and training are a must for such changes

and the compliance required and AHIMA commits to working with the industry to insure such training. Quick turnaround on any changes in this Rule will greatly assist that effort.

Again, AHIMA welcomes this opportunity to comment on the Breach Notification IFR and to continue to work with HHS, OCR,ONC, the healthcare industry, and consumers to ensure our national goals for EHRs and HIE are accomplished with maximum protections for confidentiality, privacy, and security. We hope these comments are useful, and stand ready to respond to any further questions or concerns you may have regarding these comments, or the application of confidentiality, privacy, and security requirements and practices that are the purview of the HIM profession. Please direct your questions to me at either (202) 659-9440 or dan.rode@ahima.org , or in my absence either to Allison Viola, AHIMA's director for federal affairs at (202) 659-9440 or allison.viola@ahima.org, or Harry Rhodes, AHIMA's director, practice leadership at (312) 233-1119 or harry.rhodes@ahima.org.

Our thanks for your time and consideration of these comments.

Sincerely,

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

cc. Allison Viola, MBA, RHIA – director, federal affairs
Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA – director, practice leadership