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

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

May 19, 2009

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

Ladies and Gentlemen:

The American Health Information Management Association (AHIMA) welcomes the opportunity to comment on the Department of Health and Human Services' (HHS/the Department) Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements as posted in the April 27, 2009 *Federal Register*. Our comments focus on both the Guidance as well as your questions related to Breach Notification Provisions in general.

AHIMA is a not-for-profit professional association representing more than 53,000 health information management (HIM) professionals who work throughout the healthcare industry. 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 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 rise in identity theft in the nation, AHIMA members have turned their attention to this problem and we welcome the Congress and HHS' work with regard to this issue as well. The HIM profession believes that addressing confidentiality and security is key to maintaining consumers' trust. Such trust is necessary to support the conversion to electronic health records (EHRs) and electronic health information exchange (HIE), which the HIM profession also champions.

In consultation with our members and staff experts we offer the following comments.

Response to III A: Comments on Guidance:

1. Are there particular electronic media configurations…?

Response: Electronic health or medical records (EMR/EHR) are complex and with the exception of some very small systems, EMRs or EHRs are in actuality often a compilation of systems that collect, store, and present data. We, therefore, welcome the involvement and expertise of the National Institute for Standards and Technology (NIST) both for the resources that will now be more readily available, as well as for the expertise NIST can offer to test and respond to the need for security that must be applied in these complex models and eventually in the exchange of data between and among these EMR or EHR systems through electronic health information exchange (HIE).

AHIMA recommends that the Department with the assistance of the new HIT Policy and Standards Committees continue to direct appropriate research and testing of security functions and alternatives for the benefit of the healthcare industry. Furthermore, we recommend that the Department and NIST, in alignment with the industry (as represented in the HIT Standards Committee) also solicit the expertise of other federal departments and agencies that have experience in the area of data security, so that their combined expertise might be made available to the healthcare industry for appropriate security and consumer protections, if not now, then in the future.

AHIMA recognizes that the ability to render PHI unusable, unreadable, or indecipherable to unauthorized individuals will improve or increase as HHS and industry experts apply technologies to this problem. We urge HHS to ensure that as technologies are added as alternatives or requirements, they also be directed for product certification by the Certification Commission for Health Information Technology (CCHIT). Unless individuals are trained or have access to security expertise, it is difficult to determine that a particular technology or methodology will work with a particular EMR, EHR, or similar software that may be used in relation to Protected Health Information (PHI), so the Department also needs to consider what kind of assistance and education can be given to covered entities affected by the breach requirements and not having the resources or funds for internal expertise in the area of security. This is especially true of many physician practices and other small healthcare providers and plans.

2. With respect to paper PHI, are there additional methods…?

Response: Additional methods, beyond those in the Guidance were identified as burning or chemical destruction. In our discussions on destruction it was suggested that instructions be more explicit. For instance, shredding for destruction of paper could require (at a minimum) cross-cut shredding. Members highlighted that experts have written that older shredding devices do not offer the protections of some new shredding devices. These members have suggested that HHS might want to note what will be specifically acceptable; for example: "confetti shred with a cut size of equal to or less than 0.16" x 0.31" and definitely not larger than 0.5" x 1"."

3. Are there other methods… ?

Response: We are aware that organizations also need to consider the disposal of hardware, especially computer hard drives, disks, flash drives, and similar devices. We believe the industry will welcome

guidance and education that can be added as resources in the HHS regional offices and the OCR/OESS websites. Members report that in some cases they have found Business Associates (BAs) who do not understand the importance of such security measures and in the past have balked at taking such steps. With BAs now coming under these requirements, we believe it will be necessary for more guidance and education from the Department on all forms of destruction to build both awareness and responsibility.

4. Are there circumstances under which the methods discussed [in the Guidance] would fail …?

Response: Our members with in-depth security expertise noted that the alternatives available at the NIST website are considered significant protection, but they are not 100 percent perfect. It is important for healthcare providers to have some safe harbor if such expertise is used or followed and it appears the formal guidance provided by the Department will do this.

AHIMA members suggested that as technology and methodologies improve or expand it will be important for future guidance to provide that entities holding PHI must likewise improve or expand their security processes and compliance to meet newly identified risks and system complexity. We anticipate the Department working with the industry and NIST to make security change recommendations that can be incremental for organizations to be educated in the changes, build on the technology and processes already in place, and obtain new technology in an affordable manner. AHIMA suggests that all holders of PHI complete a regular assessment of all security practices and technologies in line with the assessments called for under the HIPAA security rule.

5. Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies …? Can risk of re-identification be alleviated…?

Response: This question was interpreted as being directed toward paper-based information, since encryption and other technology can be used in electronic situations. In these paper-based cases, data is often utilized or sent with a separate identification code, especially where re-identification is potentially needed for purposes such as public health follow-up. In such a case, we believe there is sufficient protection as long as the code is kept separate (not in the hands of the receiver or user) and effectively the user then has de-identified data.

Where a limited data set is being used, truncating the birth date or zip code, as suggested in your posting, was thought to be a positive alternative. In this case, however, the question arises as to whether the identity of the provider (if situated with the data) might negate these actions.

The need for such data from providers (who have yet to have all their data in a standard digital form) is a concern that will diminish overtime. It is important not to eliminate a population from study whose healthcare providers may not have electronic health record (EHR) capacity, especially when this data collection could impact that population's overall health. We agree that the Department should consider the option suggested of limiting the birth date, and where possible truncate the zip code to 3 digits rather than 5. (Some biosurveillance studies may need to have all 5-digits to be effective.) We further believe that the use of separate identifiers (when needed) for purposes such as public health should also be permitted for the reason given above.

6. In the event of a breach…re limited data set form…concerns about notification?

Response: If the limited data set does not permit the individual or the source organization to be identified, and the birth date and zip code limits are also applied, then there should be no need for a breach notice to be required. Anytime a data security incident occurs the organization needs to initiate a process to determine and ameliorate the cause of the breach and take any other action to prevent reoccurrence.

AHIMA members are not currently aware of legal concerns regarding breach notification; however, we are currently reviewing state requirements against federal requirements and can better respond when this research is completed in a few weeks.

7. Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?

Response: Given the mixed or limited data security experience in many (and especially smaller) healthcare providers and health plans, AHIMA recommends that the Department consider ongoing education and assistance as your questions suggests. As noted above, we believe that security must become subject to EHR certification, and that certification be extended to security products that might be independent of an EHR product. Resource centers and extension centers as well as HHS regional officers should also have information available so that entities under PHI requirements have an opportunity to be educated and assisted in the procurement and use of security technology and processes that can be applied to both electronic and paper media that contain PHI. Certification of EHR and security technology would permit identification of products similar to what the Department has suggested.

Concern has been raised that the Department's guidance, over time, will change and a covered entity (HIPAA and expanded under ARRA) that qualifies in one year may not have a technology that will qualify in future years. In recognition of the need for security technology and processes to be improved or upgraded on a regular basis, we recommend the Department provide education and assistance so that covered entities understand how to increase, upgrade, or improve security in future years. It was also suggested that the Department and its extension services, or the certification agency utilize annual report documentation similar to recommendations that are published by *Consumer Reports* to specify qualified products.

Finally, it was suggested that the Department consider accreditation of the use of security processes and technology. Such accreditation could be used both to insure that adequate measures are being taken, and also to instruct those organizations who may not be using technology appropriately.

Response to III B: Breach Notification Provisions Generally:

Questions 1-3

As noted above, AHIMA is currently reviewing state breach laws and requirements against the pending federal law. We hope to have this research completed before the end of May and would be pleased to share this information with the Department.

Many of the state breach laws are new; and few healthcare providers and health plans have experienced notification or similar compliance requirements. AHIMA will be accessing its members' expertise to determine where conflicts exist that could result in multiple notices or actions being required for compliance with state and federal requirements. As with current HIPAA privacy rules, one concern of our members is the difficulty in determining which requirements are considered "more stringent" and how this might apply to the definition of and response to breach. Our members are also concerned with potential situations where multiple requirements might lead to more consumer confusion and concern.

In this discussion members also pointed out that a breach could easily cover multiple states. In reviewing the ARRA legislation these members believe the Department must provide more clarification as to how the number of individuals involved will be affect notification steps. For instance, if a breach occurs in a business associate located in Illinois, but 3 patients are from Missouri and 600 from Illinois, but the provider is in Missouri, is the "state" Illinois or Missouri? In this case would the responsibility always apply to the entity where the most individuals reside? What if the business associate resides in Iowa? These may seem to be frivolous questions, but with so many large institutions residing on state boarders, they become significant even before trying to decide which state law might cover the situation.

AHIMA has a history of providing it members and the industry with best practices related to health information practices including practices relating to confidentiality, privacy, and security. We will do so in the case of breach requirements as well. We look forward to working with HHS as well as state governments and the industry when needed to achieve understanding, compliance and consistency, as well as consumer support and trust.

Question 4: Circumstances where entities anticipate these exceptions applying?

Response: Our conversations with members identified the potential for system, "keying," or "addressing" errors that could result in availability of PHI data to staff members (and others in the same HIPAA category) that normally do not, or should not, have access to the specific data in question. We do not believe this constitutes a breach; however, staff could be required to report such an incident to the entity's privacy or security officer, who would then be charged with addressing the cause.

In our discussions of your questions, questions arose as to the language used in ARRA. For instance the phrase "able to retain such information" is vague and troubles members who will be charged to determine whether or not a breach exists. We urge the Department to consider defining such terms in preparation for the NPRM.

Conclusion

AHIMA appreciates the opportunity to comment both on the guidance provided by the Department as well as questions related to the interim final regulations. 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 Department, and the healthcare industry to ensure that these protections and other practices are actively in place.

We realize the Department has been given a short time to meet certain obligations related to breach under the American Recovery and Reinvestment Act, and if there is anything AHIMA can do to assist, please contact us. We will send further information to the Office of Civil Rights as it becomes available from our research. In the meantime, if there are any questions related to the responses 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. 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. 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