



Association of
American Medical Colleges
2450 N Street, N.W., Washington, D.C. 20037-1127
T 202 828 0400 F 202 828 1125
www.aamc.org

May 21, 2009

Charles E. Johnson
Acting Secretary
Office of Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building
200 Independence Avenue, SW
Washington, DC 20201

Submitted electronically at <http://www.regulations.gov>

RE: Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of Breach Notification; 79 Federal Register 19006

Dear Mr. Johnson:

The Association of American Medical Colleges is a not-for-profit association representing all 130 accredited U.S. and 17 accredited Canadian medical schools; nearly 400 major teaching hospitals and health systems, including 68 Department of Veterans Affairs medical centers; and nearly 90 academic and scientific societies. Through these institutions and organizations, the AAMC represents 125,000 faculty members, 75,000 medical students, and 106,000 resident physicians. The Association appreciates the opportunity to submit comments in response to the Guidance and Request for Information related to *Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of Breach Notification; 79 Federal Register 19006*.

The AAMC believes that the principles that guide the requirements for breach notification of unsecured protected health information (PHI) should be consistent with those used to develop the HIPAA security regulations. They should be: comprehensive and coordinated; scalable, so they can be effectively implemented by covered entities of all types and sizes; and not be linked to specific technologies, allowing covered entities to make use of future technology advancements.¹ The Association is concerned that the proposed approach to securing PHI does not allow for the needed flexibility that will make the implementation of a standard reasonable for covered entities and effective for individuals whose PHI is breached.

The AAMC agrees that following the guidance, including guidance for “data in use” or data in the process of being created, retrieved, updated, or deleted, should be the equivalent of a safe

¹ 68 Fed Reg 8335: February 23, 2003

harbor, thereby rendering data secure and not subject to the breach notification requirements. However, we request that HHS not consider encryption and destruction to be the exhaustive list of the methodologies and technologies that will render PHI as “unusable, unreadable, or indecipherable to unauthorized individuals.” This approach may stifle innovation and the development of other methods that may meet the same goal in the future.

The AAMC strongly supports the proposal that PHI in limited data set form should be treated as unusable, unreadable, or indecipherable. AAMC member institutions regularly use limited data sets for research and other purposes, and have been doing so since the HIPAA Privacy Rule became effective. The elements that comprise a limited data set were arrived at through extensive notice and comment rulemaking. Without substantial evidence that the limited data set as currently comprised has led to data breaches, OCR should accept that in their current format limited data sets are unusable, unreadable or indecipherable and thus not subject to breach notification requirements. Moreover, by definition, a limited data set does not include names or contact information for the individuals included in the set; subjecting limited data sets to the breach notification requirements would force covered entities to re-identify individuals in the limited data set to contact the individuals about the breach. Such a requirement puts the protected health information at additional risk of breach and poses a substantial administrative and financial burden to entities that regularly use limited data sets for research and other important purposes.

The AAMC requests that OCR not specify which off-the-shelf products meet the encryption standards, as this may result in fewer products coming to market. This could raise the price of those products that are approved, and may be a disincentive to the development of newer and better products.

If you have any questions, please contact Ivy Baer of my staff at 202-828-0499.

Sincerely,

Joanne M. Conroy, M.D.
Chief Health Care Officer