American Medical Informatics Association
The professional home for biomedical and health informatics

May 20, 2009

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

Reference: 45 CFR PARTS 160 and 164
Response to "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 Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information"

Dear Secretary Sebelius:

As the President and CEO of the American Medical Informatics Association (AMIA) and on behalf of AMIA's Board of Directors, I am pleased to submit these comments on behalf of the Association in response to the above referenced guidance and Request for Information (RFI). AMIA is the professional home for biomedical and health informatics and is dedicated to the development and application of informatics in support of patient care, public health, teaching, research, administration, and related policy. AMIA seeks to enhance health and healthcare use through the transformative use of information and communications technology.

AMIA's 4,000 members advance the use of health information and communications technology in clinical care and clinical research, personal health management, public health/population, and translational science with the ultimate objective of improving health. Our members work throughout the health system in various clinical care, research, academic, government, and commercial organizations.

As a source of informed, unbiased opinions on policy issues relating to the national health information infrastructure, uses and protection of personal health information, and public health considerations, we appreciate the opportunity to submit comments on the above-referenced guidance and RFI.

Scope of the Guidance and RFI

Section 13402 of the American Recovery and Reinvestment Act (ARRA) Pub. L. 111-5) requires HIPAA covered entities (CEs) and their business associates (BAs) to provide for notification to individuals (by CEs) and to covered entities (by BAs) in the case of breaches of unsecured protected health information (PHI).

4915 St. Elmo Avenue, Suite 401 ▫ Bethesda, MD 20814
Phone 301.657.1291 ▫ Fax 301.657.1296
E-mail: mail@amia.org ▫ www.amia.org

Section 13407 of the Act similarly provides that vendors of personal health records (PHR vendors) and certain other entities will provide notification to individuals, and third party service providers that provide services to PHR vendors will provide notification to the PHR vendor in the event of a breach of unsecured PHR identifiable health information.

As we understand it, this Guidance explains the Department's current best thinking regarding technologies and methodologies that render PHI, and PHR identifiable health information, "unusable, unreadable, or indecipherable to unauthorized individuals" – and thereby not "unsecured" PHI or PHR identifiable health information. Application of technologies and methodologies specified in the Guidance render PHI not "unsecured" and will provide a safe harbor for breach notification requirements to be issued by HHS in interim final regulations by August 17, 2009, as well as the breach notification requirements announced by the Federal Trade Commission (FTC) in a notice of proposed rulemaking (NPRM) under 16 CFR Part 318 issued on April 16, 2009. We thank the Department for issuing this Guidance, and for including a request for information regarding the breach notification provisions of ARRA in order to inform future rulemaking and anticipated updates to the Guidance.

The Guidance in Brief

The Guidance specifies two technologies that render PHI not "unsecured": 1) encryption and 2) for the media on which PHI is stored or recorded, destruction such that paper, film or other hard copy media cannot be read or otherwise reconstructed, and electronic media have been cleared, purged, or destroyed. The Department states that these two technologies or methodologies are "intended to be exhaustive and not merely illustrative" but asks for public input on whether there are other specific technologies and methodologies that should be included as ways to render PHI not unsecured.

The Guidance uses the HIPAA Security Rule definition of encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. The Guidance specifies that encryption processes tested by the National Institute of Standards and Technology (NIST) meet this definitional standard and provides specific references to NIST publications that stipulate valid encryption processes for "data in motion" and "data at rest"; NIST guidelines for electronic media sanitization are also referenced. (Future iterations of the Guidance will apply to recommendations of the HIT Policy Committee concerning the development of technologies that will allow PHI to be not "unsecured" specifically when it is transmitted within a nationwide health information network or physically transported outside the "secured physical perimeter of a health care provider, health plan, or health care clearinghouse.")

The Guidance notes that successful use of encryption depends upon two factors: the strength of the encryption algorithm, and the security of the decryption key or process – as it revises the Guidance, AMIA suggests that the Department consider including a best practice recommendation: that encrypted data and any encryption key or process be maintained separately, for instance on separate servers, in order to lessen the chances of unauthorized access to both encrypted data and the decryption key at the same time.

Setting aside for the moment the issue of the limited data set (which we will take up below), AMIA is not aware of other current alternatives to the technologies and methodologies (encryption and destruction) for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. However, we do note that in specifying these methods only, the Department has chosen to not include the alternative option articulated by Congress at Section 13402 (h)(1)(B) as a technology standard that "is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute." AMIA recognizes that in promulgating this Guidance in timely fashion, the Department was not required to include such a 'default' option. However, since neither the Department nor the other Federal information security experts it consulted can be aware of all technologies and methodologies for rendering data secure that may be developed in the future, we question whether the categorical commitment to encryption and destruction stated in the Guidance may have the effect of discouraging future innovation in information security. Further, we are concerned that in declaring encryption and destruction as the only acceptable methods for rendering PHI "not unsecured" the Guidance conflicts with the HIPAA Security rule, which provides significant flexibility – 164.306(b)(1) specifically provides that CEs **"may use any** [emphasis added] security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications of the subpart." AMIA believes the Department should give further consideration to the potential impact of specifying such an absolute standard for rendering data secure in future iterations of the Guidance.

Our thinking is mixed in regard to the Department's decision to make the Guidance effective upon issuance. On the one hand, the Guidance is preliminary to breach notification requirements that will likely not take effect until September 17, 2009, and the Department is soliciting public input on the Guidance, so it seems premature to announce that the Department recognizes PHI 'secured' by encryption or destruction as providing a safe harbor against breach reporting requirements that have not taken effect. However, the practical effect of this decision is to provide strong encouragement to CEs, BAs, PHR vendors, 3rd party service providers, and other entities to move promptly toward encrypting or securely destroying PHI (and PHR identifiable health information) whenever and wherever practicable – and AMIA strongly supports such actions as the best current methods of securing identifiable health information to the highest degree.

Consideration of the Limited Data Set as an Additional Methodology of Rendering PHI "Not Unsecured"

In developing the Guidance the Department considered whether PHI in a limited data set (LDS) should be treated as unusable, unreadable, or indecipherable to unauthorized persons for purposes of breach notification. The Department noted that including the LDS as a methodology would better align the Guidance with state breach notification laws and would mitigate administrative and legal difficulties that covered entities could face in attempting to notify individuals of a breach in light of limited contact information and requirements in data use agreements. While articulating a decision to exclude the limited data set as a methodology for securing PHI, the Guidance solicits comment on whether the risk of re-identification of an LDS warrants this exclusion and inquires about administrative and legal concerns regarding the ability to comply with breach notification requirements when direct identifiers have been removed from PHI.

AMIA believes that there are a number of compelling reasons for including the limited data set as a methodology for securing PHI and a safe harbor in relation to breach notification requirements.

First, as the Guidance notes, when an LDS is disclosed for purposes of treatment, payment, or health care operations, or as permitted or required under 164.502 or under 164.514 (e) for research, public health, or health care operations activities, the fact of the disclosure itself need not be included in the accounting of disclosures of PHI provided to an individual on request under 164.528. In establishing the limited data set as a tool to be utilized without an authorization from the individual for legitimate research, public health, and health care operations activities, then, the Department created a subset of "not fully-identifiable PHI", which not only removes direct identifiers but includes an additional mechanism, a data use agreement, that further reduces the risk that a breach of the subset would "compromise[s] the security and privacy of such information" [Section 13400 (1)(A)]. Given a previous decision to treat the LDS as "not fully-identifiable PHI" in the context of accounting for disclosures, we find it inconsistent for the Department to suggest now that the LDS is, for all intents and purposes, "fully-identifiable" PHI for breach reporting requirements.

Section 13402 (a) requires a covered entity to notify each individual "**whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been** (emphasis added), accessed, acquired, or disclosed during such breach"; Section 13402 (b) similarly outlines the requirement for business associates to notify covered entities of breaches. If – as we suggested above in recommending that encryption processes and decryption keys be maintained separately – a covered entity, in addition to including all the required elements of a data use agreement specified in 164.514 (e)(4), maintains the 'key' that could be used to re-identify individuals from the data elements included in the LDS and does not provide that key to the LDS recipient researcher or business associate, we believe that the covered entity would not have a "reasonable" belief that a breach of the LDS (which contains "not fully-identifiable" PHI) would have necessarily "compromise[d] the security and privacy" of any given individual's protected health information. At a minimum, AMIA suggests that the covered entity should be allowed to rebut that assumption via evidence, such as provided by a statistical analysis or forensic investigation, "that the information was not or could not reasonably have been acquired" [see the FTC NPRM referenced above at 318.2(a)].

The Guidance solicits feedback concerning administrative and legal difficulties that may be faced by covered entities that would be required to notify individuals of a breach of an LDS when such a breach is known to the entity. We will cite a few examples:

Section 13402 (b) requires a BA to notify a CE of a breach and to identify for the CE the individuals whose "unsecured PHI" has been, or is reasonably believed to have been, breached. If the recipient BA does not have a 'key' with which it could identify the individuals whose data elements, (not including any direct identifiers,) are included in the LDS, we are at a loss as to how the BA could, in fact, identify "each individual" as required by this section. Since the recipient BA cannot identify specific individuals within a limited data set and since a limited data set contains only data elements, such as birth date or treatment date or diagnosis, it is likely that a covered entity would have to "re-identify" all of the individuals whose data elements were contained in the LDS and send a breach notice to each of those persons, unless it makes a

determination, as we suggested above, that it does not have a "reasonable" belief that the breach compromised the security and privacy of specific individuals.

Similarly, Section 13402(f) requires covered entities to include in a breach notification a "description of the types of unsecured protected health information that were involved in the breach" and "the steps individuals should take to protect themselves from potential harm". AMIA doubts that a covered entity could adequately comply with these requirements in providing a notice of breach in relation to a limited data set. We are equally doubtful about the utility to any given individual of a breach notice saying, for example, that "a data set containing the birth dates and the dates of the first prescription filled for pain reliever X for 5,000 unique individuals was created for public health or research purposes as permitted by law and was disclosed by us (the covered entity) to a business associate (or researcher) under a data use agreement that required the recipient to have in place appropriate safeguards to prevent unauthorized use or disclosure – we (the covered entity) have been notified that the data set, and your birth date or date of first prescription filled, may have been acquired, accessed, used, or disclosed by an unauthorized person; we suggest that you should take the following steps to protect yourself from harm…"

In order to protect the security and privacy of PHI, the limited data set tool relies on the deletion of direct identifiers, execution of a data use agreement, and adherence to the minimum necessary standard found at 164.514(d). With these three requirements in place, AMIA strongly believes that the LDS should be included in the revised Guidance as a method for rendering PHI "unusable, unreadable, or indecipherable" to unauthorized individuals and should provide a safe harbor for CEs and BAs in regard to breach notification to individuals.

If the Department continues to exclude the limited data set as currently constituted from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, we recommend, alternatively, that with the removal of one further piece of information – either the month and day of birth (but not the year of birth) or the last 3 digits of a 5-digit zip code – such a limited data set would, in fact, be included and its use would provide a safe harbor for covered entities, business associates, and researchers.

Policy Implications of the Exclusion of Limited Data Sets as a Method for Securing PHI

Increasingly, health research involves queries of large data sources, including electronic health records, patient registries, claims databases, public health data sets, and the like; these multiple data environments are utilized, then, for outcomes and populations research, drug and patient safety analyses, and comparative effectiveness studies, among other things. Typically, this research does not involve fully-identified PHI but rather utilizes limited data sets.

The federal government has been strongly supportive of research using health care databases. For instance, ARRA provides $1.1 billion in new funding for comparative effectiveness research; among the stated purposes of this provision is to "encourage the development and use of clinical registries, clinical data networks, and other forms of electronic health data that can be used to generate or obtain outcomes data." Similarly, the FDA Sentinel Initiative, established by the Food and Drug Amendments Act (FDAAA) of

2007, requires the Secretary of HHS to: 1) develop methods to obtain access to disparate data sources; and 2) to develop validated methods for the establishment of a post-market risk identification and analysis system to link and analyze safety data from multiple sources, with the goals of including, in aggregate, at least 25 million patients by July 1, 2010 and 100 million patients by July 1, 2012. The language of Section 905 of the Food and Drug Administration Amendments Act – no one should "disclose individually identifiable health information when presenting drug safety signals and trends or when responding to inquiries regarding drug safety signals and trends" – clearly reflects a commitment to the use of limited data sets, rather than fully-identifiable PHI, to the widest extent possible.

AMIA is very deeply concerned that the decision of the Guidance to exclude the limited data set from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, along with several other provisions of ARRA, establish significant disincentives to the creation, disclosure, and use of limited data sets by covered entities, business associates, and researchers.

With the general prohibition against "remuneration" for PHI (which includes limited data sets) established by Section 13405(d), the requirement of Section 13405(b) that the minimum necessary principle apply to research uses of PHI (including for preparatory to research activities), and a potential interpretation of Section 13408 that would require independent researchers to become business associates, it is difficult to see why even the most public-spirited covered entity would allow for the creation, disclosure, and use of limited data sets, since to do so would expose them to the new liabilities (and untold costs) of breach reporting without any attendant benefit. Simply, the liabilities and costs of breach reporting will fall upon covered entities, and not upon business associates or researchers, even when the business associates or researchers suffer or cause the breach. With a completely unbalanced distribution of responsibilities, AMIA regretfully predicts that covered entities will move in the direction of either requiring individual authorization for data use or, alternatively, a waiver of authorization by an institutional review board (IRB). The latter option can, of course, be utilized to permit the use of fully-identified PHI, in which case more patient-identifiable data will be used, with less privacy protection than is the case today – and the limited data set will wither on the vine.

As the Department is aware, a report from the Institute of Medicine Committee on Health Research and the Privacy of Health Information concluded that the HIPAA Privacy Rule overstates the utility of informed consent to protect privacy and in not utilizing sensible privacy protections has negatively impacted the research enterprise. By analogy, we believe that the Guidance similarly ignores the opportunity to encourage not only encryption and destruction but also greater use of limited data sets as a sound principle for making protected health information more secure. AMIA requests that the Department survey covered entities on a regular basis to determine whether the use of limited data sets is declining or increasing, and the general effect of the new breach reporting requirements on health research.

Request for Information Regarding Breach Notification Provisions of ARRA

We thank the Department for the opportunity to provide comment in advance of the promulgation of breach notification requirements, as called for at Section 13402(j).

Section 13402(c) of ARRA indicates that a covered entity incurs breach reporting obligations "as of the first day on which such breach is known to such entity" entities. Having commented above about our concerns that the responsibilities for breach reporting fall primarily upon the CEs, whether or not the CE had anything to do with causing or allowing the breach, let us raise a different but related issue here. A comprehensive health record is likely to contain PHI gathered from many covered entities – in fact, this is one of the principal functions of an HIE or RHIO, to facilitate access to the many records that relate to the same individual. Now, under Section 13408 RHIOs and PHR vendors that assist CEs in offering a PHR must be business associates (BAs) of the multiple CEs that hold PHI which they routinely "access" and to which they provide data transmission. If there were an instance in which a RHIO (a BA) suffered a breach of PHI relating to one or more individuals, that RHIO would, presumably, need to notify all of the CEs that 'provided' PHI relating to a given individual – or perhaps even all the CEs with which it has contracts – and each of those CEs would in turn need to send a notice to the individual that his/her unsecured PHI was acquired, accessed, used, or disclosed in a way that compromised the security or privacy of the individual's information. Not only will this result in multiple (and confusing) breach notices being sent to the same individual, but it will put multiple CEs 'on the hook' to disclose how they will prevent such breaches in the future (perhaps by withdrawing from the RHIO or the PHR), advise the individual about steps he/she should take to prevent harm, and the like. While we appreciate the fact that a RHIO is unlikely to have any direct 'relationship' to any individual and thus is probably not a good candidate for the sending of breach notices, we think that the Department should provide additional guidance concerning the issue of the responsibilities of multiple CEs and others that may 'provide' PHI to a comprehensive record 'through' a RHIO or HIE, as well as the similar question of whether doctors, hospitals and other CEs that 'provide' PHI to a PHR would have any responsibility for notifying individuals at the point in time when it 'discovered' a breach which occurred at the PHR.

The following describes another example of the potential difficulty that a CE could face when a breach is 'discovered'. A covered entity receives federal or state funding under Medicare or Medicaid for the provision of health services. The CE discloses PHI (either fully-identified or in an LDS) to a "health oversight agency" as permitted at 164.512(d). The PHI is breached at the health oversight agency, which is neither a CE nor a BA – whether or not the oversight agency has any breach reporting obligation, (which it may under state law,) is the CE obligated under ARRA to report the breach to the individuals whose PHI was provided to the oversight agency when the CE 'discovers' (knows or should have known) the breach occurred?

In defining the term "breach" Section 13400 provides certain exceptions for unintentional acquisition, access, use, or disclosure, including when such acquisition, access, or use was made in good faith and within the scope of employment. Such an exception would 'cover' the receiver in an instance when a covered entity accidentally transmitted PHI to another covered entity. However, an inadvertent disclosure made by an authorized individual is 'covered' only when it is made to another individual in the same covered entity, and is treated as an actual disclosure (and a breach) even when made to another covered entity. To illustrate: a hospital employee inadvertently transmits prescription information to the pharmacy across the street – the pharmacy employee receives the PHI in good faith and does not further disclose it, so the pharmacy has not experienced a breach; but the hospital employee transmitted the prescription information to a separate CE (the pharmacy) and the hospital must now prepare a breach notification to be sent to the

individual whose PHI was inadvertently disclosed. Though we recognize that the Department's discretion may be limited by the language of Section 13400 here, AMIA strongly believes that an inadvertent disclosure made to another covered entity – which, of course, is covered by the Privacy and Security rules of HIPAA – should be exempted from the requirements of the forthcoming breach reporting regulation.

Recognizing that the breach notification regulations called for in Section 13402 will be promulgated by the Department, while the temporary requirements of Section 13407 that apply to PHR vendors and other non-HIPAA covered entities are under the jurisdiction of the FTC, we must point out that the significant differences between the definition of "breach" at Section 13400 and of "breach of security" at 13407(f)(1) are problematic. First, there is no logical reason that for an entity holding unsecured PHI a breach should include "unauthorized acquisition, access, use, or disclosure" of such information, while for an entity holding unsecured PHR identifiable health information a breach of security should be limited to only "acquisition of such information without the authorization of the individual". Simply, the plain language of "breach" normally encompasses the full range of unauthorized 'receivers' and 'disclosers'. Certainly, the responsibility of PHR vendors includes not actively 'disclosing' as well as preventing 'acquisition', and at the same time PHR vendors should have systems in place to prevent unauthorized 'access' or 'use'. As we believe that these differing definitions of "breach" most likely reflect a legislative drafting error, AMIA suggests that HHS and the FTC jointly seek clarification from Congress on this issue.

Summary

AMIA thanks the Department for the prompt issuance of the Guidance relating to technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. We appreciate as well the opportunity to provide input to the Department in advance of breach notification requirements that will be promulgated in a future regulation.

- We applaud the decision to recognize encryption and destruction as appropriate ways to secure PHI. We regret, however, that the limited data set (LDS) was not included as a technology or methodology for rendering PHI not unsecured, and we strongly recommend inclusion of the LDS in a future version of the Guidance.

- We are deeply concerned about the policy implications of the Department's exclusion of the limited data set as a method of rendering PHI "unusable, unreadable, or indecipherable to unauthorized individuals", and we recommend that HHS study the impact of this decision on health research.

- We are concerned that the liabilities and costs for breach reporting fall largely on covered entities, even when it is a business associate or a non-HIPAA covered entity that causes or suffers the breach. We ask for clarification of the responsibilities of the original data sources when a 'comprehensive' record, which includes PHI from multiple sources, is breached.

- We suggest that HHS and the FTC jointly request that Congress harmonize to the extent possible and practicable the definitions of 'breach' that apply to covered entities, business associates, PHR

vendors, 3rd party service providers, and certain non-HIPAA covered entities that hold PHI and PHR identifiable health information.

We applaud the Department's efforts to oversee this important national and public discourse. AMIA stands ready to work collaboratively with the Department and other organizations to address these complex public policy issues. If I can answer any questions for you, or offer additional information on this subject please feel free to contact me at detmer@amia.org or 301 657-1291.

Sincerely,

Don E Detmer, MD, MA
President and CEO