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

December 24, 2009

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

45 CFR PART 160

RIN: 0991-AB55
HIPAA Administrative Simplification: Enforcement
Interim final rule

Dear Secretary Sebelius:

On behalf of the American Medical Informatics Association (AMIA), I am pleased to submit these comments in response to the above-referenced interim final rule. 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 delivery 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 and population health, 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 clinical and personal health information, and public health considerations, we appreciate the opportunity to submit comments on the proposed rule.

AMIA thanks the Department of Health and Human Services (HHS, or the Department) for issuing this interim final rule, which amends the enforcement regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191) to conform to the revisions made pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH), which is Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5). In providing input to the Department, we will respond to the requests

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

for comment included in the information that was published in the Federal Register and discuss as well other selected provisions of the proposed rule.

General Comments

In implementing Sec. 13410 of ARRA, the interim final rule establishes three categories under which the Secretary may impose a civil monetary penalty (CMP) on a covered entity (CE) for violation of an administrative simplification provision of HIPAA:

- Violations "in which it is established that the person did not know (and by exercising reasonable diligence would not have known)" of the violation
- Violations "in which it is established that the violation was due to reasonable cause and not to willful neglect"
- Violations "in which it is established that the violation was due to willful neglect".

Sec. 13410 of ARRA also established corresponding dollar amounts of CMPs for each category of violation, as published in tabular form in the interim final rule:

TABLE 1—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

Within these ranges, "penalty determinations will be based on the nature and extent of the violation, the nature and extent of the resulting harm, as well as the other factors set forth at §160.408 (such as the covered entity's history of prior compliance or financial condition)." Timely correction of a violation could also factor into decisions of which penalty tier will apply in cases of willful neglect. Likewise, under §160.412, the Secretary may waive, in whole or part, the CMP for violations due to reasonable cause that are not corrected within the prescribed period, to the extent that the payment of the penalty would be excessive relative to the violation.

AMIA notes that the interim final rule dramatically increases the maximum penalties for violations of the Privacy Rule in which the CE has a relatively low level of fault. While retaining much of the existing structure for distinguishing between violations caused by actions at varying levels of culpability, the rule increases the maximum penalty for <u>any</u> violation to $50,000. [To give just one example of the possible impact of these increased penalties, consider a situation in which it is established that the CE did not know (and by exercising reasonable diligence would not have known) about the violation – for instance, a non-permitted disclosure or "sale" of protected health information (PHI) by a rogue employee – imposition of the maximum "did not know" penalty ($50,000) would more

than cancel out the entire financial incentive (up to $44,000 per provider) established by ARRA for the adoption and implementation of electronic health records (EHRs).]

As we read the interim final rule, HHS has almost unfettered discretion to impose large CMPs, even for violations which could not have been prevented by the CE. However, notwithstanding new definitions of *reasonable cause, reasonable diligence* and *willful neglect* at § 160.401, the interim final rule provides no guidance as to how the Department will arrive at distinctions between "did not know", "reasonable cause" and "willful neglect" – for example, if an individual does not receive a requested accounting of disclosures as called for under § 164.528 and such violation is due to a failure of the CE to provide timely training of "all members of its workforce on the policies and procedures with respect to protected health information required by the subpart" (§ 164.530 (b)(1)) will such a failure be adjudged "reasonable" because, in fact, new staff training takes place at intervals or "willful neglect" because after a number of years of HIPAA administrative simplification compliance such mistakes simply should not happen? We suggest that HHS provide additional guidance on the decision-making processes contemplated by the Department, as well as commentary regarding the imposition of minimum and maximum penalties, i.e., regarding which unknowing violations will result in CMPs of $100 (or waived completely, as permitted under §160.412), and which ones will result in CMPs of $50,000. We appreciate that §160.408 provides a list of qualitative factors that can be used to help determine the amount of the CMP, but we believe that specific examples of the Department's thinking regarding the categories of violations and the levels of CMPs it contemplates would be helpful.

In the face of significantly increased penalties for violations, AMIA encourages the Department to continue to consider the affirmative defenses outlined in § 160.410, especially when: "The covered entity establishes to the satisfaction of the Secretary that the violation is – not due to willful neglect; and corrected [emphasis added] during either: The 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply" (§ 160.410 (b)(2)). However, we do have concerns about how the Department will determine what it means for a violation to be "corrected" within 30 days – it would seem that a CE might well implement a new staff training program or administrative security procedure within 30 days, but what would it mean to "correct" a violation that is a breach, other than to comply with the requirements of new § 164.400? Must an employee who inadvertently perpetrated a breach, such as by faxing a prescription to the wrong pharmacy, be disciplined or fired? How should a CE deal with an EHR vendor whose software permitted a breach, such as reporting to the individual laboratory information that is subject to the Clinical Laboratory Improvements Act (CLIA) prohibited under § 164.524 (a)(1)(iii), in order to 'correct' the violation? Must the individual whose PHI was breached be made whole in some way?

Recognizing that in ARRA Congress both provided financial incentives to encourage providers to adopt EHR systems and called for 'stepped up ' enforcement of privacy, security and other administrative simplification provisions, including the application of punitive sanctions against CEs, AMIA believes that further explication of the Department's thinking regarding how it will find the appropriate balance

of making available technical advice and consultation while also requiring genuine regulatory compliance on the part of CEs would be invaluable. We urge the Department to go beyond the direction of Sec. 13403 of ARRA, (which provides for designation of an individual in each HHS regional office who will offer guidance and education to individuals and covered entities regarding their rights and responsibilities vis-à-vis federal privacy and security requirements relating to protected health information,) and undertake an extensive campaign to educate covered entities and business associates about the myriad changes to the existing HIPAA administrative simplification provisions that will take effect in 2010 and into the future.

We note, finally, that while the interim final rule references only CEs in regard to potential penalties for violation of HIPAA administrative simplification provisions, multiple sections of ARRA, though not yet implemented in regulation, will apply these same penalties to business associates (BAs) as well. Thus, Section 13401 of ARRA calls for the application of penalties to BAs for security violations secondary to requirements that the BA have in place adequate administrative, physical and technical safeguards, and policies and procedures, related to keeping PHI secure. Section 13404 specifically states that the privacy provisions and penalties of ARRA apply to BAs, and Section 13408 requires health information exchanges (HIEs), regional health information organizations (RHIOs) and similar entities that provide data transmission and access PHI in the normal course of business must be BAs. As the Department is expected to issue a proposed rule relating to these and many other privacy and security requirements called for by ARRA soon, AMIA urges that such proposed rule include discussion of the Department's thinking in regard the application of CMPs to business associates that undertake a wide range of covered activities.

Comments Specifically Requested

HHS has requested comments on three particular issues. The first involves the calculation of when the 30-day cure period begins for the purpose of determining the appropriate penalty tier for a violation due to willful neglect. According to Section IV.B.3 of the rule, the cure period for such purpose begins on the date the CE liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred. *Willful neglect*, in turn, is defined as "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provisions violated."

AMIA agrees that the language of the interim final rule provides a reasonable method for determining on what date the cure period begins in violations due to willful neglect. Because the cure period in such cases begins on the same day as would a cure period for a violation not due to willful neglect, the rule should be simple to apply and easy to remember. Additionally, in cases of willful neglect, it seems equitable that the CE should not get an extended cure period, but it should be charged with knowledge of the violation on the date it would have, with reasonable diligence, known about the violation.

The second issue on which HHS requested comments was whether unintended consequences might result from moving the definitions of *reasonable cause*, *reasonable diligence*, and *willful neglect* to the

new §160.401. §160.401 is located within "Subpart D – Imposition of Civil Money Penalties." As such, it should be clear that those terms are defined for purposes of CMPs, and they should be easy to find for a reader who consults the Code of Federal Regulations (CFR) to figure out how CMPs are to be calculated. Therefore, AMIA does not foresee any unintended consequences that would result from moving the definitions of the above terms to the new §160.401.

Finally, HHS requested comments on its interpretations of Congressional intent in footnotes 1 and 3. In both footnotes, HHS interprets subsections of the United States Code that have been renumbered pursuant to HITECH. HHS has assumed that Congress mistakenly referred to the subsections using the pre-ARRA numbering system. This assumption makes logical sense considering the context of the two clauses in question, and AMIA does not disagree with the Department's interpretations.

AMIA again wishes to thank the Department for issuing this interim final rule and appreciates the opportunity to submit comments. Please feel free to contact me at any time for further discussion of the issues raised here.

Sincerely,

Edward H. Shortliffe, MD, PhD
President and CEO