American Medical Informatics Association

The professional home for biomedical and health informatics

September 13, 2010

The Honorable Kathleen Sebelius
Secretary
U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, S.W.
Washington, DC 20201

Attention: HIPAA Modifications, RIN0991-AB57

Re: American Medical Informatics Association Comments to Notice of Proposed Rulemaking on Modifications to the HIPAA Privacy, Security and Enforcement Rules

Dear Secretary Sebelius:

The American Medical Informatics Association (AMIA) respectfully submits these comments in response to the Notice of Proposed Rulemaking (NPRM) on Modifications to the HIPAA Privacy, Security and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act (the HIPAA Proposed Rule), published in the Federal Register on July 14, 2010. In this response, we provide background on AMIA, offer comments regarding the proposed modifications of existing HIPAA rules, and respond to various issues raised in the NPRM.

Background

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

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

infrastructure and public health considerations, we appreciate the opportunity to submit comments on the Notice of Proposed Rulemaking referenced above.

Discussion

AMIA applauds the efforts of the U.S. Department of Health and Human Services (HHS, or the Department) to fulfill its obligations under the Health Information Technology for Economic and Clinical Health Act (HITECH) and to implement changes to the HIPAA Privacy, Security and Enforcement Rules called for in the statute. AMIA appreciates the thorough job that HHS has done to address the relevant statutory provisions in a way that will allow professionals in the field to use Health Information Technology (HIT) both efficiently and effectively.

1. Business Associates and Subcontractors

Having long argued for the establishment of a chain of trust for uses/disclosures of protected health information (PHI) related to treatment, payment, or healthcare operations, AMIA is gratified that the NPRM not only extends the requirements of the Privacy and Security Rules to Business Associates (BAs) but also to subcontractors of BAs. In our view, entities that receive, transmit, disclose or use PHI should indeed follow the Privacy Rule requirements for use and disclosure and should have security measures in place in order to keep such information confidential. Thus, AMIA also supports the extension of HIPAA rule compliance obligations to specific types of BAs, including health information exchanges (HIEs), Regional Health Information Organizations (RHIOs), and personal health record (PHR) vendors as stipulated by HITECH.

While we believe that the bar for Privacy and Security Rule compliance should be set high for BAs and subcontractors, AMIA wants to note two concerns about the operational challenges of extending the chain of trust related to use and disclosure of PHI. First, as we have commented previously, the obligation to "perform a periodic, technical and non-technical evaluation… that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart" as called for at § 164.308(a)(8) may prove significantly more burdensome for BAs and subcontractors than for covered entities (CEs). Simply, by contrast to CEs, many BAs and subcontractors may use or disclose PHI in the context of only a very small portion of their business and the costs of a full-scale (and ideally third-party) Security Rule compliance assessment may constitute a significant financial burden and could even be an impediment to innovation. Second, requiring BAs to execute 'downstream' BA agreements with subcontractors will add more layers to an already overly "rule bound" area, increasing the time and cost burden of compliance. Each new BA agreement with a subcontractor requires additional legal fees for both sides, which could represent a crushing financial obligation to some small businesses.

AMIA suggests that HHS might address these operational challenges by including new model BA contract language in the Final Rule. A model template could reduce the legal fees associated with the vast expansion of required CE to BA and BA to subcontractor contracts, and it could require BAs and subcontractors to have in place adequate administrative, physical, and technical security mechanisms without requiring the periodic assessment of § 164.208(a)(8).

2. Marketing and Fundraising

Under the current Privacy Rule, certain communications that qualify as health care operations are excepted from the definition of *marketing* and therefore do not require patient authorization. HITECH stipulated that if the CE receives direct or indirect payment for making such communications then individual authorization is required – except if the communication to the individual is about a drug or biologic currently prescribed to that person and the payment received by the CE is "reasonable" in amount. The NPRM does not clarify the meaning of "direct or indirect" remuneration, but does indicate that "reasonable" costs would be related to the CE's cost of making the communication, e.g., the cost of preparing and mailing a letter regarding a currently prescribed drug or biologic. While the statute may not allow further expansion of the exception provided for currently prescribed drugs or biologics, AMIA believes that third-party payment for other legitimate treatment communications, such as to support educational materials distributed by CEs, should be similarly exempted from the direct or indirect remuneration restriction.

AMIA supports the opportunity for patients to opt-out of fundraising solicitations. Patients should be able to opt out of all future fundraising solicitations, but we see little risk in not providing the opt-out prior to the first fundraising communication.

3. Prohibition on Sale of PHI

HIPAA appropriately permits many instances of PHI being used or disclosed for treatment, payment, health care operations, and under specified circumstances, for research, public health, and the enumerated public policy purposes. Many of these uses and disclosures are absolutely vital for uses crucial to publicly oriented goals, such as quality assessment and improvement activities, research protocol development, care coordination, evaluating provider performance, population-based activities relating to improving public health or reducing health care costs, research into breakthrough medical treatments, etc. In this context, AMIA wishes to examine the potential impact of the new § 164.508(a)(4) on the creation and use of limited data sets (LDSs) for crucial research purposes.

Today, 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 disclosure itself need not be included in the accounting of disclosures of PHI provided to an individual on request under current § 164.528. In establishing the LDS as a tool to be utilized without an authorization from the individual for legitimate research, public health, and health care operations activities, 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 prohibits any attempt to re-identify or attempt to contact individuals. Given the decision of the HIPAA Privacy Rule to treat the LDS as "not fully-identifiable PHI" in the context of accounting for disclosures, AMIA believes it is inconsistent for the Department to suggest now that the LDS is, for all intents and purposes, "fully-identifiable" PHI in regard to a prohibition of the "sale" of PHI. Thus, we suggest that new § 164.508(a)(4)(ii)(B) be modified to read:

"(B) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes, **except that such cost restrictions shall not apply when the protected health information exchanged is in the form of a limited data set as defined at § 164.514(e)(2), the disclosure is for purposes of research as permitted under § 164.514(e)(3) and the covered entity and recipient researcher have entered into a data use agreement as required at 164.514(e)(4).**"

Today, licensing, access fees or other payment arrangements support the availability of large data sets that meet the requirements of § 164.514(e)(2) or are otherwise 'partially anonymized' and are provided to legitimate researchers with carefully constructed data use agreements in place. Such remuneration certainly reflects costs incurred by the CE, which often must undertake substantial work to identify the data requested, do data extraction, do quality control to ensure that only the appropriate data is provided, perform metrics and analysis, and engage in other data processing. But cost-based fees must allow recovery of operating and capital costs if the availability of the very large data sets needed for comparative effectiveness, outcomes and quality assessment, and other crucial research, is not to be diminished. Simply, CEs will have little or no incentive to create, maintain, use and make available very large electronic data sets if their cost recovery is narrowly limited to "staff time", for instance. Thus, AMIA urges the Department to consider carefully <u>all</u> costs related to aggregating electronic PHI in general or LDSs in particular, if the cost restrictions related to research of proposed § 164.508(a)(4)(ii)(B) are included in a Final Rule.

4. <u>Research</u>

Addressing the impact of authorization requirements on research projects that combine 'conditioned' (such as enrollment in a clinical trial) and 'unconditioned' (such as agreeing to tissue banking or inclusion in a voluntary patient registry) and thereby currently require multiple consent/authorization forms, the NPRM proposes to amend § 164.508(b)(3)(i) and (iii) to allow a CE to combine conditioned and unconditioned authorizations in one *compound authorization*. AMIA supports this small but useful change to the current Rule.

We also commend the Department's stated willingness to consider the development of HIPAA authorizations that would permit future use and disclosure of PHI for research purposes, if an authorization form describes such future research activities or uses in sufficient detail to allow meaningful informed consent – and, we would suggest, a mechanism is in place to allow an individual to revoke such an "unspecified" authorization at any time. In fact, we are hopeful that the technological expertise among our members and other scientists will result in the creation of technical solutions that enhance privacy protections for patient data while simultaneously reducing the "consent" burden and easing access to data for research, quality improvement, and other uses.

Many researchers and others, including the Secretary's Advisory Committee for Human Research Protections and the Institute of Medicine, argue that as currently implemented HIPAA significantly

impedes health research. We believe that much of the claimed impediment is due to the enormous burdens relating to HIPAA 'enforcement' placed on IRBs. Echoing the NPRM's statement regarding the need for coordinated and consistent regulatory interpretation of Common Rule (45 CFR part 46) and FDA (21 CFR part 50) human subject protections, **AMIA believes that HHS should provide strong guidance and clear expectations to IRBs regarding HIPAA**. To provide one example, the Department could indicate that it expects IRBs (and attorneys advising IRBs) to exercise waiver authorities appropriately, in a way that balances potential risks to privacy and benefits of the proposed research – perhaps by developing FAQs that illuminate IRB policies and procedures for reviewing and approving, or justification for not approving, health information use for preparatory to research, retrospective, or other information-based research projects.

5. Restricting information based on self-payment

HITECH requires a CE to honor an individual's request to restrict disclosure of information to a health plan for either payment or health care operations purposes if the individual pays in full the cost of the service. The NPRM stipulates that the CE must permit the individual to choose which health care items or services a restriction applies to and the CE may not require the individual to restrict disclosures (and self-pay) for all items and services. Aside from the extraordinarily negative policy implications of this legislatively-required restriction (which encourages individuals to 'buy privacy' by not using their insurance), AMIA is concerned that there will be significant operational difficulties in trying to ensure that information systems can segregate and restrict data flows to payers. The complexities of meeting this requirement are substantial, including: CE compliance with payor contractual provisions (which often preclude charging individuals for otherwise covered services or that dictate specific rates for covered services); state law reporting requirements; quality control and fraud and abuse monitoring; design of existing clinical record systems, which generally do not allow for segmenting or flagging data based on whether they were acquired through insurance or self-pay; and the like. Further, we do not believe it is possible to develop a system in which self-pay restrictions will flow to downstream providers accurately and consistently.

6. Notice of Privacy Practices

Given that Notices of Privacy Practices (NPPs) are already exceedingly long and complicated, AMIA discourages any new additions to the privacy notice requirements, as we believe NPPs do not effectively convey information to the vast majority of patients. We believe that lengthening a complex document unnecessarily will only increase the likelihood that patients will not read it or understand their privacy options. Specifically, we do not see the "pro-privacy" value of mandating inclusion in a privacy notice of disclosures that also will require an authorization. This requirement would expand the notices for all patients or members, even where only a small minority will ever be asked for an authorization. We encourage the Department to remove the obligations to insert these new provisions into privacy notices.

7. Individual access to PHI

HITECH provided that when a CE uses or maintains an EHR, individuals have a right to obtain information within that record in an electronic format, as well as the right to direct the CE to transmit the information to a designee, such as a PHR. The NPRM broadens the right to an electronic copy of PHI from EHRs in particular to any electronic record system; thus, if the information the individual requests is maintained electronically, the CE must provide access to the information in the manner the individual requests or in another manner agreed to by the CE and the individual.

AMIA generally agrees that the current requirement that a patient be provided access to/copies of his electronic information within 30 days may be longer than should be necessary to process such requests in an electronic environment. However, we would caution HHS against adopting a timeline that would unreasonably divert healthcare providers' resources to responding to such requests. For instance, a requirement that access must be provided within five days would be unreasonable, especially if some aspect of the requested information required a physician to make explanatory notes before an administrative employee could send the information electronically.

8. Enforcement

HITECH requires that HHS must formally investigate a complaint of a Privacy Rule violation if the facts indicate possible willful neglect on the part of the CE, and must impose a civil monetary penalty if willful neglect is proven. The NPRM provides that in considering penalties, HHS will include the extent of the violation, the time period, the number of people affected, the nature and extent of harm from the violation, including reputational harm, and previous "indications of non-compliance" as well as any prior violations. We appreciate that HHS has set forth the general framework by which it would determine penalties, but we think CEs would benefit from further clarification. Specifically, in assessing violations of the HIPAA rules, HHS proposes to consider "reputational harm" to individuals and previous "indications of non-compliance" on the part of the CE, BA, or subcontractor. Because these terms are open to multiple interpretations, AMIA suggests that additional discussion of both in the Final Rule would be helpful in allowing the public to understand HHS's intent. At a minimum, providing examples of situations that might result in reputational harm and fact patterns that might indicate non-compliance would provide useful guidance.

9. Other changes

The NPRM would limit application of the Privacy Rule to a period of 50 years after death, rather than the current situation which requires the same level of privacy protection for the dead as for the living. While this is not a momentous change, AMIA believes it is a beneficial one, as data pertaining to decedents could potentially be useful for research purposes, while the possibility of causing harm through the expiration of the Privacy Rule's reach would be almost non-existent.

The NPRM would also permit CEs to disclose a child's immunization records to a school with oral consent from the child's parent or guardian, rather than the currently required written authorization, in

order to help parents comply with state laws requiring proof of immunization prior to enrolling. AMIA applauds this narrowly-tailored and worthwhile effort to reduce administrative burdens when possible.

10. Minimum Necessary guidance

The NPRM requests public comment regarding what aspects of the minimum necessary standard CEs and BAs would like HHS to address in guidance, and the types of questions CEs and BAs may have in regard to complying with the minimum necessary standard. First, AMIA believes that the confounding of LDSs with the minimum necessary data requirement contained in the HITECH legislation was not only confusing, but entirely off the mark. Simply, LDSs are constructed specifically for research purposes, while "minimum necessary" is a principle of information management. From our perspective, we believe that additional guidance regarding minimum necessary PHI uses and disclosures would be especially helpful in the area of payment activities. We submit that the Department should avoid any mandates regarding the use of an LDS.

Conclusion

AMIA again wishes to thank the Agency for issuing this Notice of Proposed Rulemaking 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