American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

September 10, 2010

Submitted electronically.

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

Re: RIN 0991-AB57; Modifications to the HIPAA Privacy, Security, and Enforcement Rues under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40868 (July 14, 2010).

Dear Secretary Sebelius:

On behalf of our more than 5,000 member hospitals, health systems and other health care organizations, and our 40,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) proposed rule on the modifications to the *Health Insurance Portability and Accountability Act* (HIPAA) Privacy, Security and Enforcement Rules under the *Health Information Technology for Economic and Clinical Health Act* (HITECH), published in the July 14 *Federal Register*. This rule implements changes to HIPAA for hospitals and other HIPAA-covered entities and their business associates.

America's hospitals are dedicated to safeguarding the privacy of patients' medical information, and the AHA and its members support HHS' efforts to implement HITECH's change to HIPAA. We generally endorse the provisions of the proposed rule. However, further improvements are needed to ensure the rule effectively serves its purpose with respect to the HITECH requirements. We also have several recommendations about the proposed changes to HIPAA provisions generally. Below is a summary of our recommendations:

- The AHA appreciates HHS' efforts to implement changes to the Enforcement Rule and supports many of the proposed changes. However, we urge HHS not to adopt its proposal to require compliance reviews where a formal investigation occurs. Also, we urge HHS to require an attempt at informal resolution of disputes except in cases of willful neglect.
- We recommend that HHS continue to permit hybrid entities to determine whether to include business associate-like activities in the health care component.
- In the interest of encouraging legitimate treatment communications, the AHA urges HHS not to impose any restrictions, such as an opt-out requirement or full authorization, for subsidized treatment communications.
- We appreciate HHS' recommended changes on the use and disclosure of decedents' information.
- We strongly urge HHS to adopt a uniform timeframe for breach notification and not to rely on a theory of agency in establishing breach notification timeframes, which we believe is particularly unworkable with the inclusion of subcontractors in the definition of business associate. We also encourage HHS to consider making the relevant provisions of the Privacy Rule directly applicable to business associates rather than relying on business associate agreements to impose such obligations.
- We suggest that HHS adopt a definition of the sale of protected health information (PHI) in order to make clear the scope of activities subject to these requirements.
- We commend HHS' proposed changes to the research authorization requirements. We believe these changes, if carefully implemented, have the potential to better facilitate clinical trial enrollment.
- We appreciate HHS' proposals to facilitate the disclosure of student immunization information. However, we encourage HHS not to require documentation of an oral agreement or to narrowly define the types of schools to which such disclosure may be made without a formal HIPAA authorization.
- We encourage HHS to permit covered entities to use and disclose department of service and patient outcomes in fundraising activities.
- With respect to the new individual right permitting request for restrictions on disclosures to health plans, we strongly urge HHS not to impose an obligation on hospitals and other health care providers to notify downstream providers of a patient's request for a restriction. We also support the adoption of an exception for disclosures required by law, as well as HHS' clarifications that: (1) a health care provider has only limited obligations to seek out-of-pocket payments that are not honored by the patient; and (2) that

information from an episode of care may be disclosed later when a patient seeks follow-up treatment without a restriction.

- We are concerned about the proposed implementation of the electronic access provisions. We urge HHS to limit this right to electronic health records, as set forth in HITECH, as well as to permit covered entities flexibility in determining available electronic formats. We ask that HHS retain the existing timeliness requirements and also make clear that a covered entity is not liable for unsecure transmissions requested by a patient, or when making reasonable efforts to verify the identity of a third party to whom a patient requests that information be sent. Finally, we appreciate HHS' proposed inclusion of labor and supply costs as permissible fees.
- We strongly urge HHS not to impose minimum necessary requirements on treatment activities, and we encourage HHS to keep in mind the importance of data for patient outcomes activities when developing any new minimum necessary guidance.

HHS has taken important steps toward ensuring that the HITECH changes are appropriately incorporated into the HIPAA rules. We believe that HHS can further improve the value of the rule for both patients and providers by making the additional refinements we recommend. Our detailed comments follow.

If you have any questions about our recommendations, please contact Lawrence Hughes, assistant general counsel, at lhughes@aha.org or (202) 626-2346.

Sincerely,

Rick Pollack
Executive Vice President

Attachment

AHA Detailed Comments on Proposed HITECH-Mandated Changes to HIPAA Regulations

ENFORCEMENT RULE

Compliance Reviews for Possible Violations Due to Willful Neglect Should Not Be Mandatory.

The AHA requests that HHS revise the proposed changes to § 168.308(a). Under HIPAA currently, the Secretary is permitted but not required to investigate complaints or conduct a compliance review to determine a covered entity's compliance with the administrative simplification provisions. HHS proposes instead to require that the department *must* conduct an investigation of any complaint and must conduct a compliance review in circumstances where a preliminary review of the facts indicates a possible violation due to willful neglect. We believe this proposal exceeds the statutory text and intent of HITECH. Section 13410(a)(1)(B) of HITECH directs the Secretary to investigate complaints where the initial facts indicate a possible violation due to willful neglect; compliance reviews are not similarly mentioned in the statutory language. Accordingly, we urge the department to revise the language of proposed § 168.308(a) to retain the Secretary's discretion to conduct compliance reviews, regardless of the perceived level of culpability of a particular entity. We believe such an approach is more consistent with the intent of HITECH, and will avoid requiring both an investigation and a compliance review in situations in which such an approach would be unnecessarily redundant.

The Resolution of Complaints and Compliance Reviews through Informal Means Should Remain Mandatory.

The AHA recommends that HHS not adopt its proposed revision to the language in § 160.312(a), which provides that the Secretary *may* attempt to resolve complaints or compliance reviews through informal means. The current regulatory text of § 160.312(a) states that the "Secretary *will* attempt to reach a resolution" of a complaint or compliance review through informal means. We believe HHS' proposed interpretation is overbroad because it makes resolution via informal means optional, regardless of the perceived level of culpability of a particular entity. Section 13410(a) of HITECH provides only that the Secretary must impose a civil monetary penalty where HHS makes a finding of a violation involving willful neglect, not for other levels of culpability, and it does not require a formal investigation for preliminary findings suggesting lessened levels of culpability. The AHA therefore urges HHS to retain the existing regulatory language, which requires at least an attempt at informal resolution for all circumstances except those involving willful neglect.

The Proposed Definitions of "Reasonable Cause," "Knowledge," "Willful Neglect" and Related Commentary Should be Adopted.

The AHA appreciates HHS' clarification of the scope of violations that fit within the definition of "reasonable cause" in proposed § 160.401. We agree with HHS' interpretation that reasonable cause may exist where, despite violating a requirement of HIPAA, an entity acted or failed to act with ordinary business care or prudence (but did not act with willful neglect). We also appreciate HHS' recognition that there may be circumstances where, despite a covered entity making a good faith effort to comply with a provision of HIPAA, a violation may occur. We agree that in these cases a violation by a covered entity is more appropriately categorized as falling within the "reasonable cause" culpability tier as opposed to the "willful neglect" culpability tier.

The AHA also supports HHS' interpretation of the knowledge standard when assessing a covered entity's or business associate's level of culpability as described in 75 *Fed. Reg.* 40878-9. We appreciate HHS' approach to considering whether an entity has compliant policies and procedures in place, as well as the entity's intent to implement the applicable HIPAA requirements in determining whether the requisite level of knowledge is present. We also agree that, when an employee acts in a manner adverse to a covered entity's or business associate's policies and procedures, the employee's knowledge of the violation should not be attributed to the entity. We believe this approach is consistent with the federal common law of agency.

With respect to willful neglect violations, the AHA commends HHS' continuation of a broad "correction" standard. In particular, we support HHS' recognition that not all violations can necessarily be fully undone or remediated. For such violations, we agree with HHS' proposed approach, at 75 *Fed. Reg.* 40879 which focuses on a covered entity's or business associate's actions to address the source of the violation (*i.e.*, implementing compliant policies and procedures when a violation is attributable to inadequate policies and procedures). We believe that a broad interpretation of "corrected" is particularly necessary in light of the distinction HHS draws in the new penalty tiers between violations due to willful neglect that have been corrected (a tier 3 penalty) and violations due to willful neglect that have not been corrected (a tier 4 penalty).

The Secretary Should Continue to Consider a Covered Entity's "Prior Violations" rather than "Indications of Non-Compliance" in Determining the Amount of a Civil Monetary Penalty.

Section 164.408 discusses the factors that the Secretary will consider in determining the amount of the civil monetary penalty to impose on covered entities and business associates. Under

HIPAA, one of the factors that the Secretary will consider is an entity's history of prior compliance, including "[w]hether the current violation is the same or similar to prior violation(s)." The proposed rule would change this factor to "[w]hether the current violation is the same or similar to previous indications of noncompliance." The AHA urges HHS to retain the current regulatory language. We believe that the proposed language is broad and ambiguous and consequently does not adequately inform covered entities and business associates of the conditions that HHS will consider in applying this factor.

HYBRID ENTITIES

HHS Should Retain Its Approach to Hybrid Entities.

Under current regulations, covered entities that are hybrid entities may include business associate-like entities (*i.e.*, entities that perform business associate-type activities) within its health care component (HCC) so long as certain policies and safeguards are in place. HHS proposes to require that a business associate-like entity in § 164.105(a) must be included within the HCC so that it is directly subject to HIPAA. The AHA requests that HHS not adopt this requirement. Under current policy, hybrid entities are *allowed* to include the business associate-like entity within their HCC but they are not required to. HHS acknowledges that hybrid entities that do not include such entities in their HCC already must establish policies and procedures to prevent uses or disclosures of PHI that would not be allowed if the business associate-like entity were within the HCC. Because of this requirement, PHI maintained by a business associate-like entity is already sufficiently protected from improper use or disclosure. In addition, as HHS notes, the larger covered entity, not the HCC, is responsible for HIPAA compliance; thus, regardless of whether the business associate-like entity is located within the HCC or not, the larger entity is always responsible for any of the business associate-type entity's HIPAA infractions.

For these reasons, we encourage HHS to allow covered entities, including hospitals, to choose whether to include their business associate-type entities within their HCCs. Regardless of whether HHS requires or merely permits this inclusion, the larger entity always will be responsible for the smaller entities' compliance with HIPAA and all of the business associate-type entity's activities will be subject to HIPAA. Therefore, PHI will be sufficiently protected if HHS allows but does not require inclusion of the smaller entity within the larger entity's HCC.

PROPOSED REVISIONS TO THE MARKETING PROVISIONS

HHS Should Adopt Its Proposed Definition of "Financial Remuneration."

The AHA endorses HHS' definition of "financial remuneration." The proposed definition provides clarity to covered entities that financial remuneration includes only direct or indirect payment from a third party whose product or services is being described. HHS' examples in the preamble further underscore this point. It is important to hospitals to be able to communicate about new services that are available to patients, such as new screening equipment, and HHS' clarification on the scope of financial remuneration will allow hospitals to conduct such communications where any remuneration is from a third party, such as a charitable organization, whose product or service is not being marketed. We further appreciate HHS' commentary at 75 *Fed. Reg.* 40885 that financial remuneration is limited to remuneration that *is in exchange for making the communication*. Again, this provides useful guidance to hospitals seeking to determine whether a particular communication requires patient authorization.

Subsidized Treatment Communications Should Not Be Subject to an Opt-out Process.

The AHA is concerned by HHS' proposal that subsidized treatment communications be subject to an opt-out process. We do not believe this approach accurately reflects the statutory language, and we urge HHS instead to permit treatment communications, regardless of whether they are subsidized, without requiring either an opt-out or full authorization. HITECH requires that communications set forth in the existing definition of marketing "shall not be considered health care operations" where the covered entity receives direct or indirect payment in exchange for making the communication, with certain exceptions. The statute does <u>not</u> prohibit characterizing these communications as treatment. Indeed, one of the exceptions in the existing definition is for treatment communications. The AHA contends that the statutory language imposes no restrictions on treatment communications, even where such communications are subsidized, and we urge HHS not to impose restrictions that will impede important and legitimate communications from providers.

In the event that HHS decides to finalize its proposal to subject subsidized treatment communications to an opt-out process, we urge the department to permit providers to narrowly tailor the scope of the opt-out to apply to communications about a particular product or service, and not to all subsidized treatment communications. Furthermore, we urge HHS not to require providers to send individuals an opt-out notice in advance of sending a subsidized treatment communication; this would add unnecessary costs for a provider without affording additional privacy protections. Finally, we ask that HHS clarify that individuals may opt back in to subsidized treatment communications using the same range of options that were available for opting out of such communications.

PROPOSED CHANGES TO TREATMENT OF DECEDENTS' INFORMATION

HHS Should Adopt the Proposed Changes to Handling of Decedents' Information.

The AHA welcomes HHS' changes relating to the protection of health information about decedents in 45 C.F.R. § 164.502(f). The change limiting covered entity responsibility for protected health information of a deceased individual to a period of 50 years following the date of death will provide helpful guidance to covered entities on how to deal with health records of the deceased. This change will reduce uncertainty related to old health records and allow hospitals to focus on securing information related to living and recently deceased patients. The AHA also appreciates the proposed amendments in 45 C.F.R. § 164.510(b)(5) that would allow a covered entity to disclose information concerning a decedent to the decedent's family members and others involved in the decedent's care or payment for that care unless doing so would be inconsistent with the prior wishes of the decedent and these wishes are known to the covered entity. Information disclosures following the death of a loved one have long been a source of frustration for families and friends, and often hospital staff cannot comply with requests for information due to HIPAA and/or state laws. These changes will make it easier for hospitals to handle disclosures of information following deaths where arrangements, such as the naming of a personal representative, were not made by the decedent prior to his or her death.

BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS

HHS Should Implement a Uniform Business Associate Breach Notification Timeframe and Specify Subcontractors' Breach Notification Obligations.

In revising the breach notification regulations to incorporate subcontractors, the AHA urges HHS to revise its guidance that when a business associate is functioning as an agent to a covered entity, the business associate's knowledge of a breach will be imputed to the covered entity for purposes of establishing when the covered entity learned of the breach. Federal common law of agency requires a detailed facts and circumstances analysis that easily could lead to differing conclusions of when an agency relationship exists. Moreover, the fact-specific determination as to whether a business associate is an agent of a covered entity must be performed for each business associate relationship. For a covered entity with thousands of business associates, this analysis would be an unquantifiable burden.

The AHA contends that abiding by the federal common law's fact-specific determination of agency is not a workable process by which to determine the applicable timeframe for breach notification. Therefore, we strongly request that HHS clarify that all business associates are governed by § 164.410(a) and its standard that a covered entity only "discovers" a breach when informed of the breach by its business associate. Applying a uniform policy would prevent the

confusion and administrative burdens that would arise under a required fact-specific determination. In the alternative, if HHS believes that an agent distinction is necessary, HHS could limit its definition of agency to certain common fiduciary relationships, such as lawyer-client and accountant-client relationships.

The AHA believes that it is particularly important that HHS implement a uniform breach notification timeframe now that subcontractors are included within the definition of "breach." Where a breach is experienced by a subcontractor who is working on behalf of a business associate agent, the covered entity for whom the business associate is an agent may have an obligation to notify affected individuals before it ever receives actual knowledge of the breach or in a very limited timeframe after it receives actual knowledge of the breach. We believe such a standard is not workable and urge HHS to implement a uniform breach notification timeframe for business associates.

With respect to subcontractors, the AHA also requests clarification from HHS regarding the notification timeframes applicable to subcontractors. We also request that in articulating subcontractors' breach notification timeframes, HHS make clear that subcontractors' breach notification obligations are to the business associates with whom they contract.

The HIPAA Rules Should Be Directly Applicable to Business Associates Rather than Rely on Business Associate Agreements to Impose Business Associate Obligations.

The AHA supports HHS' proposed modifications to the terms of business associate agreements, including that the agreements specify that business associates must: (1) comply, where appropriate, with the Security Rule provisions; (2) report to covered entities any breaches of unsecured PHI; (3) ensure that any subcontractor who creates or receives PHI on behalf of the business associate agrees to the same conditions and restrictions; and (4) comply with the requirements of the Privacy Rule applicable to a covered entity, to the extent that the business associate is carrying out a covered entity's obligations on its behalf. However, in light of business associates' new direct HIPAA compliance obligations under HITECH and the proposed rule, we request that HHS reconsider whether it remains necessary to continue to require business associates to enter into business associate agreements that impose specific contractual obligations.

Specifically, we ask HHS to consider modifying the Privacy Rule to make clear which provisions are directly applicable to business associates and to specify business associates' compliance obligations associated with each of these provisions. Such an approach would apply all of the new business associate obligations directly to business associates through the text of the Privacy and Security Rules, as opposed to relying on business associate agreements to do so. We believe that directly subjecting business associates to the applicable provisions of the rules would provide greater clarity and better facilitate compliance. It also would minimize the need

to continually revise business associate agreements following changes in the law, while ensuring that business associates are aware of and obligated to comply with all applicable HIPAA Privacy and Security Rule requirements.

Notwithstanding the above, the AHA also supports HHS' proposed business associate agreement transition period. We believe the additional compliance period is necessary to provide covered entities and business associates with sufficient time to appropriately re-evaluate and renegotiate existing business associate agreements. We also believe this approach is consistent with the previous guidance and actions of the department, such as the transition period provided for business associate agreements by HHS in the 2002 Privacy Rule.

IMPLEMENTATION OF AUTHORIZATION REQUIREMENTS FOR THE SALE OF PROTECTED HEALTH INFORMATION

The AHA is concerned that the proposed implementation of the sale of PHI provisions may unintentionally encompass a broader range of activities than was contemplated under HITECH. We believe that the intention of HITECH is to require a HIPAA authorization where there is a sale of electronic health records or PHI, and to require that such an authorization explicitly disclose that remuneration is associated with the disclosure being authorized. Instead, proposed § 164.508(a)(4) appears to encompass every authorized disclosure involving remuneration – whether or not that remuneration was in exchange for the PHI. We recommend that HHS consider implementing the sale of PHI requirements much in the way the department has implemented the marketing provisions: by defining the activity in § 164.501 and then imposing an authorization requirement in § 164.508 for disclosures that meet the definition of a "sale of protected health information." We believe this approach would appropriately preclude the sale of data – except in circumstances where an exception applies – without unintentionally sweeping in activities that do not involve the sale of data.

HHS Should Clarify the Scope of Activities Implicated by the Research Exception to Sale of PHI Authorization Requirements.

We are particularly concerned about the effect that the proposed structure for the sale of PHI provisions may have on research activities. It is imperative that covered entities fully understand the scope of activities implicated by the provisions governing the sale of PHI and that research activities other than the sale of data are clearly excluded from the authorization requirement. Hospitals routinely participate in important medical research with academics and other third party collaborators. For example, hospital IRBs may review and approve research activities, hospital physicians and other staff may engage in research directly or provide support to research activities, and research may be conducted on hospital records. There are many types of

payments involved in these research activities, such as IRB fees, staff salaries and equipment costs. These types of payments are not implicated by the HITECH requirement of a specific type of authorization for the sale of data, and it is critical that the HIPAA regulations make this clear. Any uncertainty could impede medical research. For example, an IRB that is concerned about whether it may charge its routine fee to review a waiver of authorization request that involves disclosure of data may decline to consider such requests at all. Similarly, if researchers interpret the fee restriction in research as involving more than the activity of selling data, every clinical trial authorization will now have to include the mandatory language regarding remuneration, even where none of the payments involved are for data but instead are for staff salaries and other routine research costs. Patients already find the consent process for clinical trial participation overwhelming and confusing, as the Institute of Medicine report referenced in 75 *Fed. Reg.* 40893 suggests. Further confusion that leads to including statements about remuneration where not required by the statute will only further burden research by further discouraging individuals from participating in important clinical trials.

We appreciate HHS' request for input on the types of costs that should be included in the research exception. We suggest that costs related to preparing and transmitting data includes labor, materials, related overhead, distribution, and materials. Also, the AHA supports HHS' clarification that this research exception includes limited data sets. We appreciate HHS' inclusion of limited data sets in this exception, as this clarification will be useful to hospitals who may disclose limited data sets for purposes permitted by the Privacy Rule. In the event that HHS declines to establish a definition of the sale of PHI, as suggested above, we encourage HHS to make clear that fees for an IRB review of a waiver of authorization are not implicated by the sale of PHI provisions.

HHS Should Not Impose Additional Restrictions for the Public Health Exception to Sale of PHI Authorization Requirements.

The AHA requests that HHS not include a cost-based limitation on the exception for public health disclosures. Because such a restriction would require a covered entity to evaluate any remuneration before disclosing information for public health purposes, we believe this would unnecessarily impede these types of disclosures. Hospitals routinely are asked to disclose information pursuant to § 164.512(b). For example, hospitals disclose adverse event information and engage in a wide range of required reporting related to events such as disease, injury and births or deaths. While it is not common for these types of activities to involve any type of remuneration, requiring a covered entity to determine whether any remuneration meets a regulatory standard will hinder the ability of a covered entity to make such disclosures in a timely manner.

More generally, we seek guidance on the effect that the authorization requirements for a sale of PHI have on programs for which a covered entity receives funding and, as a condition of that

funding, is required to report data. For example, under the Medicare and Medicaid incentive payment programs for hospitals and physicians that are meaningful users of certified electronic health record technology, a hospital is eligible to receive money in part as the result of reporting data to the Centers for Medicare & Medicaid Services (CMS) or a state. Similarly, a state may provide a grant to a hospital or state hospital association that is in part contingent on the reporting of certain quality data, which may include PHI. The physician quality reporting initiative (PQRI) and many health reform initiatives, such as the creation of accountable care organizations, also contemplate specific payment along with required reporting. We seek clarification from HHS that such payments are not in exchange for the sale of data and, thus, not implicated by the sale of PHI authorization requirements. We request that HHS consider establishing a new exception to the sale of PHI requirements, such as an exception for health care operations, if necessary to make clear that providers can participate in these types of programs without concerns about implicating the sale of PHI provisions.

The AHA strongly supports HHS' proposed exception to these authorization requirements for disclosures for treatment or payment purposes. We appreciate the clarification that covered entities can engage in routine activities related to the payment for health care services without concern that the sale of PHI restrictions apply.

Finally, the AHA is concerned that HHS' commentary at 75 *Fed. Reg.* 40891 that a covered entity or business associate that receives PHI pursuant to an authorization specifying that remuneration was involved may not re-disclose that PHI for remuneration without obtaining another authorization with the required remuneration language. We suggest that HHS make clear in the final rule that redisclosures of information for remuneration that are set forth in the original authorization are not restricted by this commentary. Also, in the event that HHS decides to permit a research authorization to include permission for future research studies, we request that HHS make clear that the authorization requirement for redisclosures does not apply where permission for future research is included in the original authorization.

PROPOSED CHANGES TO REQUIREMENTS FOR RESEARCH AUTHORIZATIONS

The AHA strongly endorses modifications to the research authorization regulations that would lessen the burden on research. We support the department's efforts to re-examine its approach to research authorizations. The AHA urges HHS to implement these proposals in a manner that minimizes the burden on covered entities engaged in research. Specifically, we urge HHS to allow simplified compound authorizations and to permit authorizations for future research.

The Proposed Permission for Compound Authorizations has the Potential to Better Facilitate Research.

We urge HHS to adopt its proposal to allow a single authorization to be used for conditioned and unconditioned research purposes. This would permit researchers to obtain authorization for clinical trials that include treatment, as well as to create a centralized research database or repository. As HHS notes, clinical trials frequently are combined with corollary research activities, such as the creation of a repository.

In adopting this proposal, we encourage the department to do so without imposing requirements for specific language or provisions that are unnecessarily complex and confusing to research participants, families and IRBs. Detailed regulations for statements and qualifiers regarding the various elements of a research authorization that may or may not be conditioned will result in a compound authorization being unworkable for researchers and overly confusing to patients. The AHA recommends that the department consider future modifications that will foster a more comprehensive approach to research authorizations and that better reflects the goals and approach of the Common Rule.

HHS Should Permit Authorizations for Future Research.

We believe it is critical that HHS lift the current restriction that a research authorization be study-specific, and the AHA supports the proposal in the preamble that would allow individuals to make an informed decision to authorize the use and disclosure of their PHI for future unspecified research. This revision would help to better coordinate the HIPAA rules with the Common Rule research provisions, under which an informed consent may cover both a clinical trial as well as permission for future research using the patient's information or specimens. We believe that research institutions and IRBs can, in accordance with the Common Rule, set appropriate standards for when such future research studies are appropriate and balance the public interest in the privacy of individuals' medical information with the public interest in the conduct of important medical research.

DISCLOSURE OF STUDENT IMMUNIZATION RECORDS

Covered Entities Should Not Be Required to Document an Individual's Oral Agreement.

The AHA supports HHS' proposal to amend § 164.512(b) to allow covered entities to directly disclose proof of immunization to schools in states with school entry laws. We further support HHS' decision to allow parents (or students and guardians, as appropriate) to agree in writing or orally to any such disclosures of student immunization records. We strongly believe that covered entities should be allowed to obtain either written or oral agreement. In implementing

this new requirement, however, we urge HHS not to specifically require that a covered entity document its oral agreements, but instead to provide covered entities with the flexibility to manage this process in the form they determine appropriate. A requirement by HHS that all oral agreements must be documented and the development of specific documentation standards would impose unnecessary administrative burdens on providers and would in effect eliminate any benefit provided in allowing providers to obtain an agreement orally as opposed to in writing.

The AHA requests that HHS also provide covered entities with flexibility in determining to whom to disclose student immunization records. We ask that the department not require that student immunization records only be disclosed to particular school officials identified by HHS. We believe that appropriate disclosure of immunization information will be best facilitated by giving covered entities and schools flexibility in collectively determining the appropriate individuals to receive such information.

HHS Should Not Define "School" and Should Broaden the Application of the Public Health Exception for Disclosure of Student Immunization Records to Schools.

The AHA appreciates HHS' solicitation of comments regarding whether it should incorporate a definition of "school" within the Privacy Rule. We encourage the department not to incorporate such a definition. We believe it is important for HHS to leave this term undefined because, as pointed out by HHS in the commentary at 75 *Fed. Reg.* 40895, the types of "schools" subject to school entry laws vary by state. Given the breadth of state law definitions of the term, we believe that it is likely that any definition proposed by HHS may conflict with or be inconsistent with how various state laws define the term. The AHA believes that any potential conflict or inconsistency between HIPAA and state laws may result in confusion for covered entities.

In response to HHS' request for comment regarding the scope of "schools" that should be encompassed in the proposed § 164.512(b)(1)(vi) public health disclosure exception, the AHA encourages HHS to extend the scope of the exception to include a broad range of educational institutions, regardless of whether they are subject to school entry laws. In particular, the AHA requests that HHS remove proposed subsection (B) that limits the schools to whom covered entities can disclose the student immunization records to those that are "required by State or other law to have such proof of immunization prior to admitting" an individual. We instead encourage HHS to take the position that covered entities can disclose student immunization records to all educational institutions that require proof of immunization as a prerequisite to enrollment.

FUNDRAISING

HHS Should Permit Covered Entities to Use and Disclose Department of Service and Patient Outcomes in Fundraising Activities.

The AHA also supports an amendment to § 164.514(f) to allow covered entities to use and disclose for fundraising purposes information about the department of service from which an individual received care and information about a patient's treatment outcome. It is very costly for a hospital to send fundraising communications to all of its patients rather than those from whom donations are most likely. If hospitals are able to better identify the relevance of a fundraising common to a patient, they can preserve their fundraising budgets for the patients who are most likely to donate. Allowing hospitals to use information about the departments where the patients received care and about the patient's treatment outcomes would facilitate this. Hospitals must operate on ever-shrinking margins, and fundraising is critical to their ability to provide care to every patient who needs it. If they can preserve some of their already small fundraising budgets by using treatment department and outcome information to inform their fundraising efforts, hospitals' fundraising abilities would be greatly improved.

In the proposed rule, HHS requests comments on the effect of its stricter opt-out requirement for fundraising communications. Specifically, the AHA would like to comment on HHS' proposal that the opt-out apply only to the specific fundraising campaign for which the individual requests to opt out, rather than all future fundraising communications from the entity. The AHA believes that covered entities' fundraising efforts would be unduly hampered by a requirement to remove individuals from all of their fundraising lists when the individuals only have asked to be removed from one campaign's communications.

In addition, we request that HHS issue guidance clarifying that individuals who choose to opt out of certain communications may also choose to opt back in at a later date to those fundraising communications. To ensure that neither the opt-out or opt-in process is unduly burdensome and/or costly for individuals and covered entities, we urge HHS to allow covered entities to use the same language and methods for their opt-in method as they do for their opt-out method. These methods could include toll-free hotlines and websites. We also ask HHS not to require that covered entities complete an additional step confirming an individual's desire to opt back in to such communications.

RESTRICTIONS ON DISCLOSURES TO HEALTH PLANS

There Should Be No Legal Obligation to Notify Downstream Providers.

In 75 *Fed. Reg.* 40899-900, HHS has properly identified the complexity of imposing a legal obligation on health care providers to notify other health care providers downstream of that restriction. Such an obligation would not only be almost infeasible, it also would frustrate the intent of the provision, which is to allow an individual to determine when and for which health care items and services he/she wishes to exercise the right to restrict disclosures to health plans. The AHA member hospitals strongly believe that because this is an individual right, only the individual should determine whether other downstream providers – including specialists to whom he/she has been referred, pharmacies or another hospital – should abide by the requested restriction. The election to pay out of pocket and request a restriction on disclosures to a health plan is something that a patient should discuss with each covered health care provider that he/she encounters. In addition, the AHA maintains that such a notification obligation may in fact be inappropriate in some cases, particularly in connection with services related to sensitive health conditions for which a patient does not want his/her other providers to know about the treatment he/she is receiving.

It is also important to note that currently there is no way to flag a restriction electronically so that it attaches as the information moves downstream, such as in the case of e-prescribing systems where a health care provider electronically sends a prescription for medication to a pharmacy. Furthermore, without an automated flag, it is unlikely that providers would have sufficient time to alert a pharmacy of a restriction prior to the pharmacy sending an automated benefits verification or claim to a health plan unless the provider simply did not use an e-prescribing tool and instead handed a paper prescription to the patient and placed a telephone call to the pharmacy. The administrative time and resources that would be required if HHS were to impose such an obligation on providers is significant. Even where such a restriction is technologically feasible, we believe that a patient should decide whether to exercise this right with each provider. The AHA is appreciative of the opportunity to comment on this issue and is hopeful that in the final rule, HHS makes clear that health care providers who know of a restriction in place do <u>not</u> have an obligation to notify any other providers of such restriction.

The Required by Law Exception is Important and Mandated by HITECH.

HHS has requested comment in 75 *Fed. Reg.* 40900 on types of disclosures that may be required by law and therefore excluded from any restriction on disclosures of protected health information to health plans that a provider may have in place for an individual. The AHA notes that the required by law exception is mandated by HITECH § 13405(a)(1) and believes that this exception is critical for enabling covered entities to respond to subpoenas or court orders to produce records to a health plan party to a litigation or administrative proceeding. A hospital

also may need to avail itself of this exception if protected health information that is subject to a restriction is requested for review by either the Medicare or Medicaid benefit programs as part of an audit. Such disclosures may be statutorily required.

Reasonable Efforts to Secure Payment Should Not Include Transferring an Account to Collections for Follow-Up.

HHS provided helpful commentary at 75 *Fed. Reg.* 40900 as to what a health care provider's obligations are when a patient elects to pay out of pocket and request a restriction on disclosures to his/her health plan but the form of payment is not honored. The AHA appreciates and supports HHS' guidance that in such circumstances the health care provider "may then submit the information to the health plan for payment as the individual has not fulfilled the requirements necessary to obtain a restriction." We also agree that it is reasonable for covered entities to first make some effort to resolve the payment issue with the individual before sending the information on to the health plan, but we seek further guidance from HHS that "reasonable efforts" means one to two follow-up contacts to inform the patient that his/her initial payment did not clear (*e.g.*, a check bounced or credit card charge was rejected) and that after a specified period (*e.g.*, 30-60 days), the health care provider will submit the information to the patient's health plan notwithstanding the restriction request if he/she does not provide substitute payment in that timeframe.

Even if HHS elects not to identify what would qualify as "reasonable efforts," the AHA believes it is important for HHS to clarify that "reasonable efforts" would <u>not</u> require health care providers to send the patient's account to a collection agency before being able to submit a claim to the patient's health plan. This is an undesirable step for both health care providers and for patients.

HHS' Commentary Regarding Disclosure of PHI from First Episode of Care Despite Restriction Should Be Incorporated Directly into the Regulatory Text.

The AHA commends HHS' comments at 75 *Fed. Reg.* 40900 that in cases where a patient requests a restriction on disclosure of protected health information related to an initial episode of care but fails to similarly request a restriction when obtaining follow-up treatment, the health care provider may "consider the lack of a restriction with respect to the follow-up treatment to extend to any protected health information necessary to effect payment for such treatment, even if such information pertained to prior treatment [*i.e.*, initial episode of care] that was subject to a restriction." In effect, this means that a provider may submit whatever protected health information is needed to support a claim for reimbursement to a health plan whenever there is no restriction in place related to the item or services that are the subject of the claim. The AHA thinks this clarification of the regulatory language is critical to the efficient and expeditious

management of its health care claims and encourages HHS to consider incorporating it into the regulation itself. Without the ability to submit PHI related to the initial episode of care, it is likely that many health plans would deny the provider's claim for the follow-up services at issue to the detriment of the patient and the hospital.

ELECTRONIC ACCESS

The Scope of Access Right Should be Limited to PHI Maintained in EHRs.

Section 13405(e) of HITECH provides that "in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual – the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format…" The AHA is concerned by HHS' proposal at 75 *Fed. Reg.* 40901 to expand this right of access so that it would apply "more uniformly to all protected health information maintained in one or more designated record sets electronically." For covered entity health care providers, a designated record set includes both treatment and billing records maintained by the provider. For many hospitals these records are maintained across several different systems (both electronic and paper). In order to comply with a request for an electronic copy of PHI maintained in a designated record set electronically, it would require manual identification of relevant records from each system. Many electronic systems that qualify as part of designated record set, such as billing systems, may not have functionality to easily download a subset of records for one patient electronically. Therefore, in practice, hospitals may have to resort to printing records from such systems and then scanning them to provide a comprehensive report of PHI in electronic format.

This exercise of authority by HHS exceeds the statutory directive and disregards congressional intent. In the legislative history of HITECH, the House Committee on Ways and Means noted "[t]he bill would give individuals the right to receive an electronic copy of their PHI, **if it is maintained in an electronic health record**" (emphasis added). At the time, the congressional committee cited "[g]reater use of electronic health records and other forms of health IT [which] presents an opportunity to enhance transparency and accountability within the health care system in terms of how information is used" as rationale for the provision. We encourage HHS to modify its proposal and instead adhere to congressional intent to afford individuals a right to an electronic copy of protected health information only if that protected health information is maintained in an electronic health record. To do otherwise would be too onerous for covered entities.

Covered Entities Should be able to Limit Patient Choice with Respect to Electronic Format.

HHS has proposed at 75 *Fed. Reg.* 40923 to require covered entities to provide an electronic copy of PHI in a form and format requested by the individual, if it is readily producible, "or if not, in a readable electronic form and format as agreed to by the covered entity and the individual." The AHA believes that it is reasonable for covered entities to accommodate the individual's requested format where possible but urges HHS to clarify that patients do not have unlimited choice if their preferred option is not available. We suggest that each covered entity should have the flexibility to determine the variety of electronic formats it will offer, and a patient should be required to select from those available formats if his or her preferred format is not readily producible.

The Timeliness Requirements in Existing Privacy Rule Should Remain Unchanged.

The AHA supports HHS' proposal at § 164.524(b) to apply a single timeliness standard that is consistent with the existing Privacy Rule, requiring response to an access request without unreasonable delay and no later than 30 days following the request. This approach is preferable to imposing different timeliness standards based on the manner in which the PHI is maintained. Different timeliness standards would be complicated to administer. This would be particularly true if different standards were to apply to different types of electronic designated record sets. The uncertainty as to whether a particular electronic system meets the criteria for a 30-day response time (or some other specified time period) would in itself cause delay.

Further, the AHA maintains that 30 days is necessary to make determinations about how to respond to a request no matter the format of the PHI. While providing an electronic copy of PHI maintained in an electronic health record eventually may be technologically easy, the process of determining which records are relevant and appropriate takes the same amount of time as it does for evaluating paper records. This is particularly important for hospitals where PHI related to treatment or an episode of care may not be finalized and incorporated into the treatment record until discharge. If hospitals are required to respond to requests for copies of electronic PHI in less than 30 days, the copy that is provided may not reflect the entire record. It may be missing key information that is either in transit or not yet approved and, therefore, not in the electronic systems searched in order to respond to the request.

The AHA also requests that HHS not eliminate the additional 30 days afforded to covered entities under the existing Privacy Rule to respond to a request when the PHI is maintained off-site. This is an important and necessary extension when the PHI needed to respond to a request has been archived and sent to a third party vendor for off-site storage. Hospitals generally have retention periods for electronic as well as paper data and electronic data is generally archived on back-up tapes after a designated period and sent off-site for storage, so accessing that data would not be any different from accessing paper records that are stored off-site.

HHS Guidance is Needed Regarding Requirements for Secure Transmission.

The proposed rule and associated commentary is not sufficiently clear with respect to a covered entity's obligations to ensure that the protected health information remains secure during transmission when providing an electronic copy of protected health information to an individual or his/her third party designee in one of the formats identified by HHS as acceptable. The AHA is aware that hospitals have an obligation to safeguard protected health information in compliance with the Security Rule; consistent with the Security Rule, HHS states in the preamble that "covered entities should ensure that reasonable safeguards are in place to protect the information" when responding to requests for electronic copies of protected health information. However, there are other statements in the preamble to the proposed rule that seem to indicate that if an individual requests an electronic copy of PHI in a format that is not secure, the covered entity should comply with the request so long as the individual understands the risks of unauthorized access. More specifically, HHS notes at 75 *Fed. Reg.* 40902 that "if an individual requests that an electronic copy be sent via unencrypted e-mail, the covered entity should advise the individual of the risks associated with unencrypted e-mail" instead of requiring that individual to purchase a USB flash drive from the covered entity if the individual did not have one. This example presumes that it would be more secure to download the relevant PHI to a USB flash drive and give that to the individual than it would to send an unencrypted e-mail. Nevertheless, because the individual "did not agree" to the USB flash drive format, HHS seems to be stating that the covered entity must comply with the individual's request for unsecure transmission of PHI. If that is HHS' intent, the AHA strongly encourages HHS to clarify this policy in the final rule by modifying the regulations to reflect that a covered entity would <u>not</u> be found to be non-compliant with its Security Rule obligations and would not be found to have caused a breach of unsecured PHI if it were to transmit PHI in an unsecure manner after specific request by the individual to send it in that manner and after advising the individual of the potential risks of unauthorized access during transmission.

HHS Should Maintain Existing Flexible Approach for Verification and Should Clarify that Disclosures to Third Parties Designated by Individual Patient Request do not also Require a Valid HIPAA Authorization.

In the proposed rule, HHS emphasizes that "whether the process [for receiving requests to transmit a copy of PHI to a designee] is electronic or paper-based, a covered entity must implement reasonable policies and procedures under § 164.514(h) to verify the identity of any person who requests protected health information, as well as implement reasonable safeguards under § 164.530(c) to protect the information that is used or disclosed." The AHA supports this statement and urges HHS to maintain the same flexible approach that is in the existing Privacy Rule to allow each covered entity to establish reasonable verification procedures that will work for its business rather than prescribing a standard verification procedure that must be followed by all covered entities.

With respect to requests from individuals to send an electronic copy of PHI to a person that he or she designates, HHS has proposed in § 164.524(c)(3)(ii) that the request must "be in writing, signed by the individual and clearly identify the designated person and where to send the copy of protected health information." Based on this proposal, it is apparent that the written request does not rise to the level of a valid HIPAA authorization. Accordingly, the AHA seeks amendment of the regulations to reflect that covered entities may disclose an electronic copy of PHI to a third party designated by an individual upon the individual's request without a valid HIPAA authorization if the request satisfies the criteria specified in proposed § 164.524(c)(3)(ii).

The Inclusion of Labor and Supply Costs is Appreciated.

The AHA appreciates the department's proposal that both labor and supply costs may be accounted for in the reasonable cost-based fee charged to individuals for providing an electronic copy of protected health information. In particular, the AHA member hospitals anticipate that they will incur labor costs that are directly related to reviewing and responding to requests and that such costs may not be negligible as HHS expects. For example, the anticipated labor costs include administrative staff time to review several different electronic systems that make up a designated record set to identify the relevant PHI. The AHA also commends HHS' proposal to permit the inclusion of the cost of supplies such as CDs, flash drives or other portable media in the reasonable fee charged to an individual if the individual requests such a format. The costs of such media are not insignificant, and it will be important to hospitals to be able to pass those costs on whenever an individual does not provide the necessary supplies.

MINIMUM NECESSARY

HHS Should Consider the Data Needed for Patient Outcomes Activities.

Section 13405(b)(1)(B) of HITECH requires HHS to take into account "the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease"[1] as it develops minimum necessary guidance. The AHA requests that HHS consider the fact that, over time, the amount of information necessary to accomplish these goals will increase because health reform initiatives require greater access to data. For example, accountable care organizations, quality initiatives, and continuity of care initiatives each will require the reporting and analysis of an increasing amount of data. Therefore, the AHA urges HHS to take into account these broader needs for data as it develops its minimum necessary guidance.

[1] HITECH Act § 13405(b)(1)(B).

HHS Should Preserve the Current Treatment Exception.

The AHA asks HHS to preserve the existing exception for treatment disclosures in any future minimum necessary guidance. Currently, uses and disclosures for treatment are not subject to the minimum necessary standard, and we strongly believe that it is critical for hospitals that this exception be maintained. If disclosures for treatment purposes were subject to the minimum necessary standard, patient care and safety could be jeopardized by a lack of information that does not meet the minimum necessary standard but is in fact ultimately essential to a patient receiving proper treatment. Because hospitals are large entities in which dozens of professionals may work together on a single patient, it is very difficult to predict which information will be most useful for each specialist or other professional to have, and thus the minimum necessary standard would make it impossible for hospitals to release limited information without exposing themselves, their employees, and their patients to the risk of inaccurate or inadequate care. In particular, emergent care situations require physicians and other professionals to have a patient's information as quickly as possible, and requiring hospitals to apply the minimum necessary standard here would pose a grave harm to the patient.

HHS Should Not Require Consideration of a Limited Data Set.

In addition, as HHS issues its minimum necessary guidance, we urge the department not to require covered entities and business associates to first determine whether a limited data set (LDS) is feasible as the minimum necessary amount of data before applying its own minimum necessary standard. This requirement would create a tremendous burden for covered entities and business associates through the added work involved in analyzing the limited data set and the time and money lost when this step is taken in addition to applying the minimum necessary standard. Because LDS are not used frequently, it does not make sense to require covered entities and business associates to conduct the analysis, as it most often will require unnecessary effort and utilize scarce resources.