

September 13, 2010

The Honorable Secretary Sebelius  
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, SW  
Washington, DC 20201

**RE: Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; 45 CFR Parts 160 and 164; RIN: 0991-AB57**

Dear Secretary Sebelius:

We the undersigned organizations appreciate the opportunity to submit comments on the Department of Health and Human Services' (HHS) proposed rule on modifications to the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules as prescribed in the Health Information Technology for Economic and Clinical Health Act (HITECH) of the American Recovery and Reinvestment Act of 2009 (ARRA), which was signed into law on February 17, 2009.

Privacy and security of patient health information is a principle that physicians take very seriously. It is imperative that strong privacy and security standards and protections be in place to avoid unauthorized use or disclosure of unsecured protected health information (PHI). At the same time, **privacy and security safeguards should be practical, flexible, and affordable for physicians and other health care providers with varying levels of technical sophistication to implement, and should not hinder the necessary flow of health information for treatment, payment, and health care operations purposes.** As physicians continue to move toward with the adoption of electronic health records (EHRs) and the nation transitions to electronic exchange of health information, it is important that the privacy and security practices for protecting patient information do not unduly compromise the ability of clinicians to operate their practices or care for their patients. **Overreaching privacy and security requirements and enforcement mechanisms could severely hamper our nation's move towards improving patient care and reducing inefficiencies through the use of EHR technology.**

Extension of Compliance Deadline

HHS recognizes that HIPAA covered entities, including physicians, and their business associates (BAs), will need sufficient time beyond the effective date of the final rule to comply with the requirements of the final rule. HHS proposes to provide covered entities and BAs up to 180 days beyond the effective date of the final rule to comply with most of the rule's provisions. **While we support HHS' extension of the effective date of the**

**final rule, we recommend that HHS extend the compliance date for implementation of new or modified HIPAA standards and implementation specifications to a minimum of 1 year beyond the effective date of the final rule.** The final rule will require covered entities and their BAs to review and amend their privacy and security practices and programs. Physicians and other affected health care providers will have to devote significant resources to incorporating HIPAA modifications required under ARRA and the final rule to their privacy and security practices. The Privacy Rule has not been amended since 2002, and the Security Rule has not been amended since 2003. This unfunded, mandated overhaul of the HIPAA requirements will involve significant time, money, and efforts, especially for small physician practices. Physicians are already devoting substantial resources towards EHRs and compliance with existing laws, including rules stemming from the health system reform law, the “Patient Protection and Affordable Care Act” (ACA). **To ensure optimal compliance, we strongly urge HHS to extend the compliance deadline a minimum of 1 year beyond the effective date of the final rule to allow ample time for compliance with modifications to HIPAA standards and implementation specifications.**

#### Business Associates (BAs)

BAs are required to directly comply with the HIPAA privacy and security requirements. HHS proposes to expand the definition for BAs to cover: Patient Safety Organizations (PSOs) and patient safety activities; Health Information Organizations (HIOs); E-Prescribing Gateways; or other persons that facilitate health data transmission services and routinely access protected health information (PHI); and vendors of personal health records (PHRs). Subcontractors of BAs, defined as non-BA workforce members who act on behalf of the BA, would also need to comply with the HIPAA requirements. We support HHS’ expansion of the BA definition and inclusion of subcontractors. BAs and subcontractors should be required to enter into BA agreements to ensure compliance with the HIPAA Privacy and Security requirements. HHS should make considerable efforts to educate BAs regarding their direct accountability under HIPAA. **We believe that any individual or entity involved with the creation, receipt, collection, storage, maintenance, or transmission of PHI that impermissibly uses or discloses unsecured PHI should be held directly accountable.**

#### Compliance with Federal and State Privacy and Security Laws

Physicians must comply with both federal and state privacy and security laws. It is extremely burdensome for physicians to assess whether federal privacy law overrides state privacy laws or vice versa. This is especially challenging for physician and other health care provider organizations located in multiple states, each with different privacy laws. Physicians are not legal experts and should not be expected to understand the legal nuances between federal and state privacy and security laws. **We strongly recommend that HHS work with states to identify any state laws that conflict with the new HIPAA requirements and urge states to conform their inconsistent or conflicting laws with HIPAA privacy and security requirements.**

## Amendment to the HIPAA Enforcement Rule

HHS proposes to continue to seek to resolve complaints and compliance reviews (except for willful neglect cases) through informal means. **We strongly support providing HHS with discretion to resolve HIPAA concerns through informal means. Informal processes should be flexible enough to accommodate proof of compliance, completed corrective action plan(s), or any other agreement between HHS and the affected covered entity or BA.**

**We also support HHS' proposal to consider the nature and extent of an alleged HIPAA violation as well as the nature and extent of the harm in determining the amount of any civil money penalty for a HIPAA violation.** As electronic technologies and electronic exchanges of health information will be used more frequently, HHS should work with physicians and other health care providers to disseminate information on how best to use encryption and similar technologies to secure PHI and to ensure EHRs and other technologies used by physicians (e.g., smart phones and laptops) incorporate appropriate security measures.

With the exception of willful neglect cases, we encourage HHS to pursue corrective action plans in lieu of levying fines for situations where the covered entity or BA did not know, or by exercising reasonable diligence would not have known, of a violation. We also support the preclusion of HHS from imposing civil penalties (except in cases of willful neglect) if the violation is corrected within a reasonable length of time from the date that the covered entity or BA knew, or, by exercising reasonable diligence, would have known that the violation occurred.

We believe there will be very few cases of willful neglect. We do not want the threat of excessive fines or enforcement activity that could financially devastate small businesses to, for example, act as a deterrent to the widespread adoption and use of EHRs. Rather than impose arbitrary and excessive civil penalties, **HHS should commit to working with covered entities and their BAs who have experienced a privacy or security failure to develop and implement corrective action. In addition, HHS should ensure that appropriate low cost security technology is available in the marketplace to protect PHI from impermissible uses and disclosures.**

We are also concerned about duplicative investigations and fines regarding the same alleged violation. The proposed rule indicates that if HHS determines that more than one covered entity or BA was responsible for a violation, HHS will impose a civil money penalty against each covered entity or BA. If the alleged violation was caused by the BA (and not the covered entity), then the fine, if warranted, should be levied against the BA, not the covered entity. **Fining two parties for the action of one is unfair and unreasonable. For example, if a physician's billing vendor does not disclose the loss**

**of the vendor’s unencrypted laptop that contains unsecured patient health records to the physician in a timely manner, the billing vendor should be held solely responsible for the HIPAA violation. Moreover, if the subcontractor of the BA (e.g., laptop vendor) was the cause of the PHI being unsecured (e.g., failed to properly implement encryption technology), the BA’s subcontractor (not the covered entity or BA) should be solely responsible for the HIPAA violation.**

#### Minimum Necessary Standard

ARRA requires HHS to issue guidance on what constitutes the minimum necessary amount of information for purposes of the HIPAA Privacy Rule. The minimum necessary standard requires covered entities and BAs to limit uses and disclosures of, and requests for PHI to “the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.” Since covered entities and BAs are directly accountable for impermissible uses and disclosures of PHI and subject to civil and criminal penalties for noncompliance, the exchange of PHI among these parties for treatment, payment, or health care operations activities should continue to be permissible. Covered entities and BAs are in the best position to assess if they should apply minimum necessary or limited data set policies and procedures to meet the needs of a particular use, disclosure, or request in question. Holding the party responsible for the HIPAA violation accountable for the impermissible use or disclosure of unsecured PHI is a better solution than impeding the exchange of health information for necessary health system functions like those for treatment, payment, and health care operations. **We strongly urge HHS to develop guidance that does not obstruct in any way the use and disclosure of PHI among covered entities and BAs for treatment, payment, or health care operations purposes.**

#### Health Care Operations Definition

HHS proposes amending the definition of “health care operations” to include a reference to patient safety activities, as defined in the Patient Safety and Quality Improvement Act of 2005. **We support the expansion of the health care operations definition to include patient safety activities and patient safety organizations (PSOs), since many physicians are participating in patient safety initiatives which involve the use of PHI.** HHS should also keep in mind that physicians who use EHRs will have to provide an accounting of disclosures, including ones on health care operations, to a patient upon request, which will be extremely burdensome for physician practices. HHS should consider the challenges that physicians will face when developing regulations on the accounting of disclosures and should consider extending the compliance deadline for this new requirement.

#### Modifications to BA agreements and Notice of Privacy Practices (NPP)

We appreciate HHS’ recognition of the administrative burden and costs that covered entities and BAs will face as they implement amendments to BA agreements in order to comply with the new HIPAA requirements. We strongly support the HHS proposal to

allow covered entity/BA/subcontractor written agreements to continue to operate for up to 1 year beyond the compliance date of the new requirements. We also support the proposal to deem contracts to be compliant with the modifications to the HIPAA Rules until either the covered entity or BA has renewed or modified the contract following the compliance date of the modifications, or until the date that is one year after the compliance date, whichever is sooner. In cases where a contract renews automatically without any change in terms or other action by the parties (e.g., evergreen contracts), HHS proposes allowing evergreen contracts to be eligible for the extension and deem them to be compliant. We support this and **urge HHS to expedite the availability of sample amendments/addendums to BA agreements, that could permit existing contracts to comply with the new HIPAA requirements. In addition, we urge HHS to produce a sample BA agreement template that covers all of the HIPAA requirements, including the final HIPAA modifications.**

**We also recommend that HHS expedite the availability of a sample Notice of Privacy Practices (NPP) amendment/addendum that could permit existing NPPs to comply with the new HIPAA requirements. We agree with HHS' recommendation that physicians should only have to make the revised NPP available upon request to a patient and make it available in their office in a clear and prominent location (e.g., waiting room of a physician practice).**

#### Research

We support the HHS proposal to streamline the process for obtaining an individual's authorization for research by allowing a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. These provisions would allow covered entities to combine authorizations for scenarios that often occur in research studies. For example, a covered entity would be able to combine an authorization permitting the use and disclosure of PHI associated with a specimen collection for a central repository and authorization permitting use and disclosure of PHI for clinical research that conditions research-related treatment on the execution of a HIPAA authorization.

In addition, when an entity currently requests authorization for using PHI for research, the specific parameters under which the researchers are permitted to use this information must be clearly outlined for the individual. HHS is considering whether to modify its interpretation that an authorization for the use or disclosure of PHI for research be research-study specific. HHS is proposing to allow: 1) an authorization for uses and disclosures of PHI for future research purposes to the extent such purposes are adequately described in the authorization; 2) an authorization for future research only to the extent the description of the future research included certain elements or statements specified by the Privacy Rule; and 3) option #1 as a general rule but require certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities, such as research involving genetic analyses or

mental health research, that may alter an individual's willingness to participate in the research. **We urge HHS to actively solicit feedback from those in the medical research field regarding whether HHS' privacy requirements would impose substantial administrative, financial, and legal burdens to covered entities that regularly use health information for research, public health, and other important purposes. It is also important to assess whether these types of enhanced authorization forms would present a barrier to individuals taking part in research efforts, such as clinical trials.**

#### Disclosure of Student Immunization Records to Schools

HHS proposes allowing covered entities to disclose proof of immunization to schools so long as the covered entity obtained verbal approval from a parent, guardian, or other person acting *in loco parentis* for the individual, or from the individual him/herself, if the individual is an adult or emancipated minor. HHS also proposes that once a student's immunization records are obtained and maintained by an educational institution or agency to which the Family Educational Rights and Privacy Act (FERPA) applies, the records are protected by FERPA, rather than the HIPAA Privacy Rule. **We support HHS' proposal to permit covered entities to release proof of immunization to a school if the covered entity obtained verbal approval from a parent, guardian, or other person acting *in loco parentis* for the disclosure.**

#### Right to Request Restriction of Use and Disclosure of PHI

ARRA requires that when an individual requests a restriction on disclosure of his/her PHI, the covered entity must agree to the requested restriction, unless otherwise required by law, if the request for restriction is on disclosures of PHI to a health plan for the purpose of carrying out payment or health care operations, and if the restriction applies to PHI that pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full. HHS requested feedback regarding whether physicians should be held responsible to inform other health care providers (e.g., a pharmacist, specialist) of the patient's request. **We strongly object to physicians being required to inform other health care providers of the requested restriction. A request for restriction should be made directly by the patient to subsequent health care providers. A physician has no control over the privacy and security practices of subsequent health care providers, and should not be held responsible for uses and disclosures of PHI outside his/her control. In addition, if a patient's check is returned for non-payment or if a patient refuses to pay in full up front at the time of service for a service or claim, the physician must have an unrestricted right to submit the service or claim to the health plan for reimbursement.**

HHS also notes that if a person places a restriction on the disclosure of PHI to a health plan regarding certain services, visits his/her physician for follow-up treatment, asks the physician to bill the health plan for the follow-up visit and does not request a restriction at the time nor pays out of pocket for the follow-up treatment, then there should be no restriction in effect with respect to the initial and follow-up treatment(s). Health plans

will undoubtedly require physicians to submit information about the original treatment to the health plan so that the plan can determine the medical appropriateness or medical need of the follow-up care provided to the individual. **We urge HHS to indicate in the final rule that if an individual does not request a restriction on the disclosure of PHI pertaining to a follow-up service, and the patient does not pay in full, out-of-pocket for this follow-up service, then the restriction to the prior treatment no longer applies. In addition, we urge HHS to clarify whether the right to restrict the use and disclosure of PHI extends to Medicare and Medicaid patients.**

It is also important to keep in mind that many contracts between health care providers and health plans require physicians to submit claims for all covered services. The compliance deadline should take into account that these contracts will need to be amended by the health plans to allow a patient's right to restrict uses and disclosures of their PHI to the health plans.

#### Access of Individuals to PHI

ARRA requires that when an EHR is being used by a covered entity, the individual has a right to obtain from the covered entity a copy of his/her information in an electronic format and may also ask the health care provider to transmit this information to the individual's designee so long as this is clearly communicated. The law also permits the covered entity to charge a fee for this information but it can not be any greater than the labor costs in responding to the request for the copy. Furthermore, the law calls for the covered entity to provide the information in the form or format requested by the individual when feasible. **We urge HHS to provide as much flexibility as possible in defining what constitutes a "reasonable" fee. We assert that this fee should cover reasonable labor, office supplies, retrieval, and copying costs associated with preparing, copying, and transmitting these medical records in an electronic format. In addition, we support HHS' recommendation not to bind covered entities to electronic standards that may not yet be technologically mature, and to provide covered entities with the flexibility to provide their patients a readable electronic copy in a format determined by the covered entities in order to meet this requirement.**

Existing HIPAA law requires providing a patient access to their medical information within 30 days from the date of the patient's request, and also authorizes an extension period up to an additional 30 days. **We support a single timeliness standard that would include PHI stored on paper and in electronic systems, rather than having multiple standards based on practice capabilities and system capacity.** In today's physician practice environment, interfaces between EHRs and electronic patient portals are not readily available. Requiring complex and expensive electronic patient portals is simply untenable, especially for smaller practices. Physicians adhere to strict standards for communicating medical information to patients. These standards include the issues of timeliness, related directly to the criticality of the information, and the personal communication of difficult information. All communication depends on physician's knowledge of the condition of the patient, an assessment of their current treatment plan,

the impact of the information on the patient, as well as other factors. **Physicians must have the discretion to make these determinations based on the physician-patient relationship. Physicians and patients are in the best position to determine what records are needed and when they are needed.** Physicians should also have the discretion to discuss test results with their patients prior to labs sharing them with patients. Patients could receive information that is confusing or unanticipated lab results (e.g., confusion over medical terminology to describe results or diagnostic tests indicating poor prognosis) that may cause undue anxiety if the clinician does not have sufficient opportunity to clarify and translate results with their patients. Physicians must be able to provide health information in a form and within a timeframe that will be useful and acceptable to the patient. **The current HIPAA requirement to provide a patient access to their medical information within 30 days from the date of the patient's request, and that authorizes an extension period up to an additional 30 days, should remain in place as the standard for both paper and electronic records.**

#### Restrictions on Marketing, Sale, and Fundraising Activities that Involve PHI

HHS proposes modifications to the definition of “marketing.” Certain communications to individuals about health-related products or services would now be considered marketing communications requiring an individual’s authorization, if the covered entity receives financial remuneration by a third party to make the communication. We support the provision that face-to-face communications regarding products or services between a covered entity and an individual and promotional gifts of nominal value provided by a covered entity do not require a written authorization by the patient. We also agree with the HHS clarification that communications made by a covered entity to individuals promoting health in general, such as communications about the importance of maintaining a healthy diet or getting an annual physical, are not considered to be marketing activities. Similarly, we agree that refill reminders and other communications about a drug or biologic that is currently being prescribed would not require individual authorization. An authorization would not be required if any financial remuneration the covered entity receives from the manufacturer is reasonably related to the covered entity’s cost of providing the notification. We support the provision that covered entities would also be permitted to receive financial remuneration in exchange for making a treatment communication to an individual, if the covered entity’s NPP includes a statement that it may make such communications, and that the communication includes disclosure of the remuneration and an option for the individual to opt out of future communications.

ARRA prohibits the sale of PHI without an individual’s written authorization, a requirement which is effective six months after publication of the final rule. There are several exceptions to the authorization requirement. These exceptions are when the purpose of the exchange of information for remuneration concerns: (1) public health activities; (2) research if the price charged for the information reflects the costs of preparation and transmittal of the data; (3) treatment of the individual (HHS proposed that this exception also cover payment purposes); (4) the sale, transfer, merger, or consolidation of all or part of a covered entity and for related due diligence; (5) services rendered by a BA pursuant to a BA agreement and at the specific request of the covered

entity; (6) providing an individual with access to his or her PHI; and (7) other purposes determined by the Secretary of HHS. HHS proposes that an authorization include a statement that the covered entity is receiving direct or indirect remuneration in exchange for the PHI. HHS has also proposed that if PHI is disclosed for remuneration by a covered entity or BA to another covered entity or BA, the receiving covered entity or BA could not redisclose the PHI in exchange for remuneration unless a valid authorization is obtained with respect to such redisclosure.

HHS proposes a number of changes to the Privacy Rule's fundraising requirements to comply with ARRA, including: (1) strengthening the opt out by requiring that a covered entity provide a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications; (2) clarifying that the covered entity would not be permitted to condition treatment or payment for care on an individual's choice of whether to receive fundraising communications; and (3) clarifying that a covered entity may not send fundraising communications to an individual who has elected not to receive such communications. **We encourage HHS to develop easy to follow guidance that would describe varying circumstances whereby a covered entity must obtain an authorization from an individual due to a marketing, sale, or fundraising activity that involves PHI. We strongly recommend that HHS put together guidelines that include common examples of sales, marketing, and fundraising activities that require authorization versus those that do not require an authorization.**

#### Education and Outreach

**We recommend that HHS conduct comprehensive outreach and education initiatives so that physicians and other health care providers, patients, BAs, subcontractor BAs, and other affected parties fully understand the new HIPAA requirements and responsibilities, including when notifications and authorizations are required and what types of technology are recommended to secure PHI.**

#### Conclusion

Constant vigilance to privacy and security concerns is imperative to preserve the rights and trust of patients. This vigilance, however, should not become a barrier to the goal of electronic exchange of health information and widespread EHR adoption and use. Educating covered entities, BAs, and their subcontractors, as well as the public, on reasonable and affordable measures to ensure the privacy and security of PHI and compliance with the new HIPAA requirements is an important, critical step for minimizing improper uses and disclosures of patient information. The AMA along with the undersigned organizations appreciate the opportunity to comment. Should you have any questions about our comments please direct them to Mari Savickis at [mari.savickis@ama-assn.org](mailto:mari.savickis@ama-assn.org) or 202-789-7414.

Sincerely,

American Academy of Dermatology Association  
American Academy of Facial Plastic and Reconstructive Surgery  
American Academy of Family Physicians  
American Academy of Neurology Professional Association  
American Academy of Ophthalmology  
American Academy of Otolaryngology – Head and Neck Surgery  
American Association of Clinical Endocrinologists  
American Association of Neurological Surgeons  
American Association of Orthopaedic Surgeons  
American College of Cardiology  
American College of Chest Physicians  
American College of Emergency Physicians  
American College of Osteopathic Internists  
American College of Osteopathic Surgeons  
American College of Physicians  
American College of Radiology  
American College of Rheumatology  
American College of Surgeons  
American Congress of Obstetricians and Gynecologists  
American Gastroenterological Association  
American Geriatrics Society  
American Medical Association  
American Osteopathic Academy of Orthopedics  
American Osteopathic Association  
American Society for Clinical Pathology  
American Society for Radiation Oncology  
American Society for Reproductive Medicine  
American Society of Cataract and Refractive Surgery  
American Society of Clinical Oncology  
American Society of Hematology  
American Society of Plastic Surgeons  
American Thoracic Society  
College of American Pathologists  
Congress of Neurological Surgeons  
Heart Rhythm Society  
Infectious Diseases Society of America  
Medical Group Management Association  
Renal Physicians Association  
Society for Cardiovascular Angiography and Interventions  
Society for Vascular Surgery  
The Endocrine Society