September 13, 2010

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, 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:

The Medical Group Management Association (MGMA) appreciates the opportunity to submit comments on the Department of Health and Human Services' (HHS) proposed rule, "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act."

MGMA, founded in 1926, is the nation's principal voice for medical group practice. MGMA's more than 22,500 members manage and lead 13,700 organizations, in which more than 275,000 physicians provide more than 40 percent of the healthcare services delivered in the United States. MGMA's core purpose is to improve the effectiveness of medical group practices and the knowledge and skills of the individuals who manage and lead them.

MGMA supports comprehensive privacy and security standards to avoid unauthorized use or disclosure of unsecured protected health information (PHI). It is critical that as an increasing number of physician practices migrate to electronic health records (EHRs) and other technology, there be sufficient protections in place to ensure the privacy and security of patient data. However, with such diversity of practice size and composition, technology, and human and capital resources, it is critical that the privacy and security safeguards mandated by the government practical, flexible and affordable for each of these organizations. Overly stringent and rigid requirements could have the unintended consequence of hindering the necessary flow of health information for treatment, payment and health care operations purposes.

HEADQUARTERS
104 Inverness Terrace East
Englewood, CO 80112-5306
phone: 303 799 1111
fax: 303 643.4439

GOVERNMENT AFFAIRS
1717 Pennsylvania Avenue
North West, Suite 600
Washington, DC 20006
phone: 202 293 3450
fax: 202 293 2787

www.mgma.com

## Extension of compliance deadline

Issue:

Recognizing that HIPAA covered entities and their business associates (BAs) will need sufficient time beyond the effective date of the final rule to comply with its requirements, 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.

Recommendation:

**MGMA supports the extension of the effective date of the rule and requests that HHS extend the compliance date even longer, from 180 days to at least one year after the final rule becomes effective. This added time is necessary to give practices an opportunity to fully evaluate and make the needed modifications to their privacy and security policies. With passage of the American Recovery and Reinvestment Act (ARRA) and, shortly after, the Patient Protection and Affordable Care Act, medical group practices are expending considerable resources to stay abreast of the new requirements placed on them by these laws. Medical groups and other covered entities will need to devote significant additional resources, time and money to incorporate HIPAA modifications into their privacy and security practices. This will be especially true for small physician practices. We strongly urge HHS to extend the compliance deadline to a minimum of one 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)

Issue:

Under ARRA, BAs will be required to comply with the HIPAA privacy and security requirements. HHS proposes to expand the definition of 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, will also need to comply with the HIPAA requirements.

Recommendation:

**MGMA supports HHS' expansion of the BA definition and its inclusion of subcontractors of BA. BAs and subcontractors should be required to enter into BA agreements to ensure compliance with the HIPAA privacy and security requirements but a subcontractor should be liable even when a BA has failed to enter into a BA agreement with the subcontractor. 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 and responsible for the impermissible use or disclosure of unsecured PHI should be held directly accountable.**

Compliance with federal and state privacy and security laws

Issue:

Covered entities and their business associates face a complex analysis to determine the provisions of state and federal privacy and security laws, with which they must comply. In certain instances, federal privacy and security requirements will preempt state law, while in other cases, state law is deemed to be more stringent and therefore also remains enforceable. In still other instances, a state may have applied for and received an exception to the preemption requirement. This analysis is extremely burdensome, especially for practices 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.

Recommendation:

**We strongly ecommend that HHS work with states to identify any state laws that conflict with the new HIPAA requirements and 1) urge states to conform their inconsistent or conflicting laws with HIPAA privacy and security requirements; and 2) provide educational materials to assist healthcare providers in determining the state privacy and security requirements that differ from, or are in addition to, the federal requirements.**

Amendment to the HIPAA Enforcement Rule

Issue:

HHS proposes to continue to work with covered entities and seek to correct indications of noncompliance through informal means, except in circumstances that indicate a possible violation due to willful neglect. HHS also proposes to modify the regulations relating to civil money penalties to expand liability to BAs in the same manner it applies to covered entities, as mandated by ARRA.

Recommendation:

**MGMA supports the agency's goal of seeking compliance through voluntary corrective action as opposed to formal enforcement proceedings. With the exception of willful neglect cases, for which a formal investigation is statutorily mandated, we urge the agency to work with covered entities and BAs to understand the requirements of this revised rule and, where a potential violation has been alleged, to work with those entities to develop an appropriate corrective actio plan.**

**The agency appropriately expands its rules to BAs in its modifications to 45 C.F.R. § 160.402(c). MGMA urges the agency not to impose a fine on a covered entity when the BA is responsible for the violation and has had a fine levied against it for the same alleged violation. If the alleged violation was caused by the BA (and not the covered entity), then the fine, if warranted, should**

Minimum necessary standard

Issue:

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."

Recommendation:

**The exchange of PHI among these parties for treatment, payment or healthcare operations activities should continue to be permissible between covered entities and their BAs. We strongly urge HHS to develop guidance that does not hinder the use and disclosure of PHI among covered entities and BAs for treatment, payment or healthcare operations purposes.**

## Healthcare operations definition

Issue:

HHS proposes amending the definition of "healthcare operations" to include a reference to patient safety activities, as defined in the Patient Safety and Quality Improvement Act of 2005.

Recommendation:

**MGMA supports the expansion of the healthcare operations definition to include patient safety activities and patient safety organizations (PSOs). However, we encourage HHS to consider the impact of this expansion on the new accounting of disclosures requirements for practices that utilize an EHR. HHS should extend the compliance deadline appropriately to ensure sufficient time for the marketplace to develop EHR software that can account for these types of disclosures.**

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

Issue:

Recognizing the administrative burden and costs that covered entities and BAs will face when amending BA agreements to comply with the new HIPAA requirements, HHS proposes to allow current covered entity/BA/subcontractor written agreements to continue to operate for up to one year beyond the compliance date of the new requirements. It also proposes 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, or until one year after the compliance date, whichever is sooner. In cases where a contract renews automatically without any change in terms or other actions by the parties (e.g., evergreen contracts), HHS proposes allowing evergreen contracts to be eligible for the extension and to deem them compliant.

Recommendation:

**MGMA supports this extension to amend BA agreements. We urge HHS to make available sample amendments/addendums to BA agreements to 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 do not believe that the requirements of 45 C.F.R. § 164.520(c)(2)(iii) requiring**

**a revised NPP to be posted and available upon request would be overly burdensome for healthcare providers.**

## Research

Issue:

HHS proposes streamlining the process for obtaining an individual's authorization for research by allowing a covered entity to combine conditioned and unconditioned authorizations for research. The authorization must clearly differentiate between the conditioned and unconditioned research components and clearly allow the individual the option to opt in to the unconditioned research activities

Recommendation:

**Prior to making any final determinations, MGMA urges HHS to solicit input from medical research stakeholders regarding whether HHS' proposed privacy requirements would impose substantial administrative, financial and legal burdens to those that use health information for research, public health and other 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

Issue:

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.

Recommendation:

**In order to facilitate efficient communication of immunization records, MGMA supports the 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

Issue:

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 healthcare operations. The restriction applies to PHI that pertains solely to a healthcare item or service for which the healthcare provider involved has been paid out of pocket in full. HHS requested

feedback regarding whether physicians should be held responsible to inform other healthcare providers (e g., a pharmacist) of the patient's request.

Recommendation:

**MGMA does not support requiring a covered entity to inform other healthcare providers of the requested restriction and believes the responsibility for such a request should remain with the patient. A physician has no control over the privacy and security practices of subsequent healthcare providers, and should not be held responsible for uses and disclosures of PHI outside his/her control.**

**Further, a physician must have the right to submit a claim to a health plan in the event that the 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**

**With respect to follow-up care, MGMA agrees with HHS's assessment that if a patient asks a physician to bill a health plan for follow-up treatment and does not request a restriction at the time nor pay out of pocket for the follow-up treatment, 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.**

**We also note that many contracts between healthcare providers and health plans require physicians to submit claims for all covered services. For this reason, we believe that additional time is needed for compliance to allow time for such contracts to be amended.**

Access of individuals to PHI

Issue:

ARRA requires that when a covered entity uses an EHR, an 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 cannot 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.

Existing HIPAA law requires covered entities to provide 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

Recommendation:

**MGMA urges HHS to provide as much flexibility as possible in defining what constitutes a**

"reasonable" fee. This fee should include 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.

MGMA believes it is most appropriate to have a standard 30-day time period (as well as the extension period up to an additional 30 days) for covered entities to produce a patient record that would include PHI stored on paper and in electronic systems, rather than having multiple standards based on practice capabilities and system capacity.

In addition, it is clear that Section 13405(e) of the HITECH Act does not require the covered entity to produce information in the electronic format requested by the individual. Rather, the Act requires only that the individual shall have a right to obtain a copy of such information in an electronic format from the covered entity. The proposed rule addresses only how a request can be handled if both parties agree and provides no guidance on how this can be addressed if both parties do not agree to the information being delivered in a PDF format. We urge HHS not to include in the final rule a requirement that a covered entity produce the record in the form and format requested by the patient. At a minimum, the final rule should clarify that, if the patient's requested form and format cannot be met by the covered entity, the covered entity be permitted to provide the information to the individual in a PDF format.

Restrictions on marketing, sale and fundraising activities that involve PHI

Issue:

As required by HITECH, HHS proposes modifications to the definition of "marketing," prohibits the sale of PHI without a patient's written authorization except in limited circumstances and sets forth changes to the fundraising requirements.

Recommendation:

MGMA anticipates that these new requirements have the potential to cause confusion as healthcare providers attempt to understand when authorizations are required. We strongly request and recommend that HHS provide easy-to-use and detailed guidance for covered entities to assist in compliance efforts.

Education and Outreach

In order for physician practices to fully understand the new HIPAA requirements and responsibilities, we recommend that HHS launch a comprehensive set of outreach and education initiatives. These should be targeted to ensure that healthcare providers, patients, BAs, subcontractor BAs and other impacted stakeholders fully understand the new HIPAA regulations.

Conclusion

In conclusion, MGMA is a strong supporter of patient access to and protection of their health

information. We are concerned, however, that overly burdensome privacy and security requirements will hinder the critical flow of clinical and administrative data to authorized recipients. Onerous bureaucracy that does little to protect patient information clearly runs counter to the goal of decreasing healthcare costs and increasing efficiency through administrative simplification. We look forward to continuing to collaborate with HHS on privacy and security issues.

Thank you for the opportunity to comment on this important proposed regulation. Should you have any questions regarding our comments please contact Robert Tennant at rtennant@mgma.org or 202-293-3450.

Sincerely,

William F. Jessee, MD, FACMPE
President and CEO