June 6, 2022

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Electronically submitted via www.regulations.gov

Re: Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act (RIN 0945-AA04)

Dear Secretary Becerra,

On behalf of our member medical group practices, the Medical Group Management Association (MGMA) is pleased to provide comments to the U.S. Department of Health and Human Services (HHS) in response to the "Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended" request for information (RFI) regarding certain provisions from the HITECH Act.

With a membership of more than 60,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,000 medical groups in which more than 350,000 physicians practice. These groups range from small private practices in rural areas to large regional and national health systems and cover the full spectrum of physician specialties and organizational forms.

As cyberattacks have escalated in recent years, particularly aimed at healthcare organizations, MGMA acknowledges it is critical for medical groups to take steps to protect patient health information and secure their clinical and administrative electronic systems. MGMA has worked diligently to educate medical groups on cybersecurity best practices, but even the most proactive and prepared practices can fall victim to an attack. In a recent MGMA poll, 16% of medical groups reported experiencing a cyber or ransomware attack in 2021.[1] Group practices are becoming more vigilant and taking precautions to protect themselves and the patients they treat, such as incorporating cyberinsurance policies, conducting HIPAA Security Risk Assessments, encrypting all files and systems containing patient information, training employees on cybersecurity, and more.

MGMA supports the efforts of HHS to better understand what recognized cybersecurity practices medical groups have voluntarily implemented and offers the following recommendations as the agency potentially moves forward with future rulemaking.

Summary of Key Recommendations

- **Allow flexibility. MGMA recommends** HHS continue to recognize the broad statutory definition of the term "recognized security practice" to ensure physicians have the flexibility

[1] MGMA *Stat*, February 15, 2022

to choose their own recognized security practices, as there are vast differences in the technical and financial capabilities between medical groups of all sizes.

- **Offer best practices and education.** Sample frameworks or checklists would offer real-world approaches for medical groups to implement acknowledged cybersecurity policies into their practices.
- **Harmonize regulations with other programs. MGMA recommends** HHS take steps to ensure potential requirements are consistent with other programs such as rulemaking by the Office of National Coordinator for Health Information Technology (ONC) to prohibit "information blocking," as defined by the 21st Century Cures Act.

Detailed RFI Comments

Public Law 116-321

HHS Question: What recognized security practices have regulated entities implemented? If not currently implemented, what recognized security practices do regulated entities plan to implement?

MGMA Response: Medical groups have implemented security programs such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Health Industry Cybersecurity Practices, in addition to working with lesser-known vendors or vendors tied to electronic health record (EHR) systems. Each medical group has unique needs. Unfortunately, it is possible that smaller groups may not have a recognized security practice due to their need to balance security efforts with the administrative burdens and costs associated with currently recognized programs.

MGMA urges HHS to prioritize flexibility when it comes to which security programs medical groups should implement. We are concerned that a mandate for groups to adopt specific recognized security systems would lead to unintended consequences stemming from increased costs and administrative burden. Medical groups should be in the driver's seat to appropriately balance the need to protect protected health information (PHI) with their ability to stay financially viable and avoid interruptions to patient care.

MGMA recommends HHS not mandate what constitutes recognized security practices beyond what Congress intended. Regulated entities should implement security programs based on practice size, complexity, infrastructure, and the costs of the security measures. HHS should accept, not limit, the broad statutory definition of the term, "recognized security practices." There are a variety of scenarios that may not be accounted for should HHS mandate certain security practices, such as programs that are already included in practice management systems (PMS) or EHRs. Medical groups should be allowed to continue using their professional judgment as to what is best for their practice and the unique situations they face. For many groups, the most financially viable or available option would be to bundle cybersecurity and cyberinsurance with the PMSs or EHRs they already utilize.

HHS Question: The Department requests comment on any additional issues or information the Department should consider in developing guidance or a proposed regulation regarding the consideration of recognized security practices.

MGMA Response: As cyberattacks can occur at any point in time, it is essential that medical groups ensure security practices are in place to protect health information and mitigate interferences on effectively delivering high-quality care. The statutory definition for "recognized security practices" is purposefully broad and we believe HHS should continue interpreting it in a manner that ensures medical groups are able to choose the security program that best fits their specific needs.

MGMA requests that HHS offer best practices and education that medical groups can reference to understand how to best protect their practices from cyberattacks. Real-world guidance, such as offering a sample framework or a checklist of sample policies would offer ways for medical practices to stay financially viable, while continuing to implement cybersecurity policies into their practice.

MGMA urges HHS to harmonize regulations with other programs such as the information blocking rule by ONC as defined by the 21st Century Cures Act. There is a need to harmonize current and future regulatory frameworks for which medical groups must comply. We are aware that ONC will soon release regulations and penalties pertaining to data blocking. ONC information blocking rules penalize physicians for not sharing health information, but on the other hand, HIPAA penalizes physicians for sharing too much information. To prevent unnecessary confusion and burden on medical groups, HHS should consider other rules and policies impacting physicians while developing additional regulations.

MGMA urges HHS to consider good faith efforts undertaken by medical groups to ensure security practices are in place. If HHS moves forward with a regulatory proposal, the agency should take into consideration good faith efforts made by medical groups to demonstrate that security practices were in place for the previous 12 months should it intend to levy civil monetary penalties or monetary settlements on regulated entities.

As the voice of the country's medical group practices, MGMA remains committed to promoting policies that enhance the ability of our members to provide high-quality, cost-effective care to the millions of patients they serve. MGMA appreciates the opportunity to provide feedback to HHS. Should you have any questions, please contact Swapna Pachauri at spachauri@mgma.org or 202-293-3450.

Sincerely,

/s/

Anders Gilberg
Senior Vice President, Government Affairs