December 16, 2019

The Honorable Diana DeGette
2111 Rayburn House Office Building
Washington, DC 20515

The Honorable Fred Upton
2183 Rayburn House Office Building
Washington, DC 20515

Re: CURES 2.0 Legislation

Dear Representatives DeGette and Upton:

The Medical Group Management Association (MGMA) is pleased to submit the following response to your request for comment on health information technology (HIT) legislation. Streamlining electronic access to health information will assist both clinicians and patients make informed healthcare decisions, decrease administrative costs for physician practices and improve the care delivery process for patients. We commend you both for taking on the task of developing legislation to modify and augment the 21st Century Cures Act of 2015.

MGMA is the premier association for professionals who lead medical practices. Since 1926, through data, people, insights, and advocacy, MGMA empowers medical group practices to innovate and create meaningful change in healthcare. With a membership of more than 55,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,500 practices of all sizes, types, structures, and specialties that deliver almost half of the healthcare in the United States.

Interoperability

- **Require ONC to develop a pathway to address security concerns in APIs and apps.** While MGMA supports the use of Application Programming Interface (API) to enhance interoperability and give patients access to their health information, we are concerned about the security implications with the deployment of APIs. Absent appropriate privacy protections, we believe patient information is at risk of being sold, used for vendor marketing, and shared without permission with third parties.

  Patients must be the primary authority in designating rights to access, exchange, and use of their data, but practices have a role to play as well. ONC must design a process that gives practices the assurance that a third-party application has met a minimum level of security.

  ONC must ensure patients are educated on the rights, responsibilities, and to the potential threats to their data. API technology suppliers that capture, store, or transmit health information should be required to: (i) conduct surveillance and mitigate threats and vulnerabilities that could be introduced to an information system to which the API could connect; (ii) be certified by an ONC-recognized third-party accreditation entity (i.e., The Electronic Healthcare Network Accreditation Commission) as meeting a minimum level of privacy and security requirements; and (iii) give informed consent via a standardized app acknowledgement process for any use of their health information by a third-party app. Apps should also be required to provide to consumers statements regarding how the data

will be used by the developer and whether data will be disclosed or sold to other entities.

- **Require third-party app developers sign BAAs.** To better ensure that appropriate security measures are in place, ONC should require healthcare app developers to obtain a business associate agreement (BAA) with practices and other HIPAA covered entities. A BAA would create a safe harbor from liability should health information be disclosed by a third-party and was not authorized by the patient.

- **Create simplified, understandable, and actionable definitions for EHI and name USCDI as the baseline.** The ONC proposed rule defines electronic health information (EHI) too broadly, which will lead to significant confusion in the industry and also to potential enforcement action against providers. ONC should be required to establish the United States Core Data for Interoperability (USCDI) standard as the baseline definition of EHI that would apply for purposes of information blocking.

- **Require ONC to eliminate complex information blocking requirements.** MGMA recognizes the importance of limiting information blocking, but the approach proposed by ONC is far too complex. It would significantly increase administrative burden for physician practices, cause industry confusion regarding what data can be disclosed and when and increase the risk for sensitive health information to be shared inappropriately or not shared when needed.

  Rather than subject providers to information blocking penalties, ONC should be required to conduct a comprehensive educational campaign to better inform clinicians and their patients regarding their rights and responsibilities vis-à-vis information exchange. Information blocking requirements should be reasonable, actionable, and not add needless administrative burden.

- **Narrow the HIN Definition.** ONC's definition of a Health Information Network (HIN) is vague and could be broadly interpreted to include healthcare entities that would unfairly be required to comply with ONC mandates. The definition of HIN should be narrowed to encompass only those entities that are actual health information networks and have a specific operational role and responsibility for the network.

- **Increase EHR oversight.** ONC should be required to conduct comprehensive oversight of EHR software and employ "real-world" testing. Physician practices need assurance that the software they purchase meets the requirements set out in the ONC certification. ONC should be instructed to ramp up its surveillance of health IT vendors for compliance with ONC certification requirements, security protocols, and appropriate fee charges.

- **Establish out-of-pocket cost transparency.** MGMA supports the call for price transparency. However, simply requiring providers to disclose their walk-in charges for common procedures is not the solution. Patients are increasingly responsible for co-insurance payments based on a percentage of the charges allowed under their insurance plans, so it is essential that they know the amount their insurance will pay for services received. HHS should be directed to develop or support real-time benefit tools that provide accurate out-of-pocket costs at the point of care and incentivize physician practices to implement these tools.

- **Establish a staggered implementation timeline process.** ONC should be directed to first establish a reasonable timeline for software vendors to develop and deploy the next CEHRT edition or software requirement. Next, ONC should establish a reasonable

timeline for clinicians and other providers to be required to use any new CEHRT edition or health IT in federal health IT and/or quality reporting programs. This staggered implementation approach would ensure a smooth transition to new standards and requirements and decrease the potential of rushed technology implementations that lead to patient safety issues and additional administrative burdens and cost for physician practices.

- **Expand HITAC representation**. The Health Information Technology Advisory Committee should be expanded to include additional representatives from the physician practice community. Participants should represent different sizes of groups, different medical specialties, and organizations with varying levels of technology implementation.

- **Require HHS to use discretion in its initial enforcement of information blocking, prioritizing education and corrective action over monetary penalties.** Prioritizing education will be more effective over the long-term in ensuring physician practices are compliant as they will better understand the regulatory requirements.

Quality Payment Program and Certified EHR Technology

- **Exclude those not participating in the QPP from mandates requiring CEHRT.** ONC should be directed to not require clinicians who are ineligible for participation in the Quality Payment Program (QPP) to be subject to any mandates that require CEHRT. At a minimum, these clinicians should be given 24 additional months to comply.

- **Permit use of non-certified EHR technology.** Allow eligible clinicians to use non-certified health IT that works for their specialty and patient population to count toward their QPP scoring.

- **Health IT credit beyond CEHRT.** Allow eligible clinicians to receive high-weight credit for use of health IT beyond CEHRT in the QPP.

Appropriate Use Criteria

- **Repeal the AUC requirement in PAMA.** The requirements for capturing and reporting the Appropriate Use Criteria (AUC) data will impose a significant administrative burden and cost on both the ordering and furnishing professionals. The outcome of this onerous reporting process identifies only 5% or less of outlier ordering professionals. We believe that the intent of the Protecting Access to Medicare Act (PAMA), passed in 2014 prior to the enactment of the Medicare Access and CHIP Reauthorization Act of 2015, can be achieved through alternative approaches.

  The AUC provision of PAMA should be repealed and CMS should be instructed to: (i) Use the principles and intent of MACRA to guide cost reduction and value-based activities; (ii) Increase the multi-category MIPS weight for consultation of Clinical Decision Support Mechanism (CDSM) software in the Improvement Activities, Quality, Cost, and Promoting Interoperability components of MIPS; (iii) sponsor AUC conferences, webinars, and other forms of professional education (i.e., offering CEUs for physicians) to discuss the clinical and economic value of CDSM consultation; (iv) offer multiple CDSM options free of charge to ordering professionals; and (v) work with the appropriate medical specialty societies and professional associations such as MGMA, with emphasis on primary care physicians, to focus on educational opportunities, distribution of evidence-based research, and distribution of free CDSM tools.

Hospital Admit, Discharge, Transfer

- **Permit intermediaries to transmit ADT notifications.** CMS should be directed deem a hospital compliant if they send the Admit, Discharge, Transfer (ADT) alerts to an intermediary such as a HIE to distribute to their provider networks.

- **Permit multiple ADT notification transmission options.** HHS should be directed to permit hospitals to have multiple options to comply with the proposed ADT notification requirement so they may pick the best option for working with their community providers. As the process of sending ADT notifications matures, work may need to be undertaken by standards-setting bodies like HL7, convened by ONC, to develop a more robust standard that would support the sharing of additional data points, including those outlined by CMS in the proposed rule.

- **Align ADT notifications with information blocking.** CMS should be required to work closely with ONC to align the ADT requirement with the information blocking component of the ONC regulation.

Patient Matching

- **Require CMS to work on the issue of patient matching.** One of the most critical challenges for the healthcare industry is accurately identifying the patient and tying that identification to the appropriate medical record held by an authorized healthcare entity. Even though it was identified as a critical issue in HIPAA and that legislation called for a national patient identifier, the industry does not yet have a standardized, unique patient identifier. We contend that successful interoperability, the exchange of electronic healthcare information, will be extremely difficult to achieve across the nation's healthcare ecosystem in the absence of a cost-effective and accurate method of matching patients to their records.

  Identifying the patient correctly is essential for healthcare providers, insurance providers, and others exchanging data for both clinical and administrative purposes. Most importantly, patient care is improved, and patient safety is enhanced when health information is accurately transmitted between healthcare entities, especially in emergency situations. Accurate patient matching is critical if physician practices are to rely on the data transmitted to them. To improve patient matching, CMS should be required to work with appropriate industry stakeholders in addressing the issue of the accurate and appropriate matching of patient records.

- **Standardize patient demographic data.** To improve patient matching, we recommend ONC support the standardization of demographic data, including applying the U.S. Postal Service Standard to the address field. We also encourage exploring the use of email address as an additional patient matching element.

Conclusion

In conclusion, MGMA supports the objective of deploying HIT in physician practices to improve the sharing of clinical data to improve the care delivery process decrease administrative burdens. However, considerable work must be accomplished to overcome the numerous technical, legal, and logistical barriers to the widespread and effective use of health IT. Through implementation of updated Cures legislation, appropriate regulatory policies, processes, and incentives, as well as outreach to physician practices and other key stakeholders, we believe that the nation's health IT

infrastructure can achieve the original goals and vision laid out in the 2015 Act.

We look forward to continuing to work with your offices to facilitate physician practice transition to effective and efficient health IT and ensure that the promise of improving the nation's healthcare through the use of national standards becomes a reality. Should you have any questions regarding these comments, please contact Robert Tennant, Director, Health Information Technology Policy, at 202.293.3450 or rtennant@mgma.org.

Sincerely,

/s/

Anders Gilberg, MGA
Senior Vice President, Government Affairs