May 4, 2021

Robinsue Frohboese
Acting Director
Office for Civil Rights
U.S. Department of Health and Human Services
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

RE: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement (RIN 0945-AA00)

Dear Acting Director Frohboese:

The Medical Group Management Association (MGMA) is pleased to submit the following comments in response to the Department of Health and Human Services (HHS) Office for Civil Rights' (OCR) notice of proposed rulemaking on "Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement."

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 60,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,000 group medical practices ranging from small private medical practices to large national health systems representing more than 350,000 physicians.

We are supportive overall of OCR's efforts to modify the HIPAA Privacy Rule to provide patients greater access to their medical records and to remove regulatory barriers to individual-level care coordination and case management while continuing to protect the privacy of patient health information. Nevertheless, MGMA is concerned that providing increased access to protected health information (PHI) with fewer guardrails, particularly around organizations outside the purview of HIPAA, will have unintended consequences for the security and privacy of patient data. We are also cautious about increasing access rights in ways that have the potential to substantially increase the administrative burdens placed on medical practices or create scenarios in which medical practices are more likely to face penalties due to the infeasibility of complying with more stringent requirements.

Key Recommendations

MGMA appreciates the opportunity to submit the following key recommendations in response to the proposed rule:

- **Allow clinicians to use their professional judgement in deciding when to allow patients to take photos or videos of their PHI at the point of care.** MGMA opposes a blanket mandate to always afford patients this right of access without delay when PHI is readily available at the point of care.

- **Maintain the current 30-day timeline to fulfill patient requests for access to their medical record, including an optional 30-day extension with written notice**. Shortening this timeline in the current environment would make compliance infeasible for many medical groups and disproportionately penalize small and independent practices.

- **Withdraw the mandate that would require covered entities to act upon oral requests to share electronic PHI with third parties.** While MGMA supports removing unnecessary barriers for individuals seeking to exercise their access rights, we are concerned that such a mandate could have unintended consequences and lead to erroneous disclosures of sensitive patient information. The option to submit such disclosure requests electronically through patient portals is a more desirable alternative.

- **Maintain the ability of healthcare providers to charge a cost-based fee in cases where a patient directs the transmission of an electronic copy of PHI in an EHR or a non-electronic copy of PHI through other than an internet-based method to a third party.** If OCR finalizes a permitted fee structure, that structure should recognize the difference in cost when manual labor is required to meet a request.

- **Finalize the proposal to eliminate the requirement for a covered entity to obtain a written acknowledgement of the Notice of Privacy Practices (NPP)**. There is no practical use for this acknowledgement, and we believe removing this requirement will reduce administrative burden. The proposed content revisions to the NPP should be captured in a model NPP created by OCR and easily adaptable by medical practices.

In addition to our recommendations pertaining to key substantive provisions of the proposed rule, MGMA is concerned with the timing of these proposed changes to the HIPAA Privacy Rule in the context of two overarching circumstances impacting the medical practice landscape at present: the ongoing COVID-19 pandemic and the regulations implementing the 21st Century Cures Act, in particular the final rule promulgated by the Office of the National Coordinator for Health Information Technology (ONC), heretofore referred to as the ONC information blocking rule.

Medical groups continue to feel the impact of the COVID-19 pandemic, especially in the areas of practice operations and staffing. Many practices are still heavily reliant on telehealth to administer care to their patients, which continues to create workflow challenges for practices operating on a "hybrid" telehealth and in-office visitation model. Additionally, given over a year spent in the pandemic, many practices are suffering from low morale, high burnout, and challenges with adequate clinical and administrative staffing. As practices continue to grapple with these and other challenges for the foreseeable future, implementing changes to HIPAA will require additional staff time and divert critical resources from patient care at a time when patient care should be paramount. **For this reason, we urge OCR to reconsider implementing significant changes to the HIPAA Privacy Rule in the midst of the COVID-19 public health emergency.**

At the same time, medical groups have recently been tasked with implementing significant workflow and process changes in order to comply with the ONC information blocking rule. The compliance date for the earliest provisions of this rule began in April 2021, and further compliance and effective dates will continue through 2022. Complying with the ONC regulation already requires the prioritization of substantial technological and administrative resources as medical practices adjust how they respond to patient and third-party requests for electronic health information (EHI) and develop new policies and procedures to comply with the rule. **Given this policy area is already in flux due to previously finalized regulations implementing the 21st Century Cures Act, we urge OCR to refrain from effectuating any modifications to the HIPAA Privacy Rule prior to the full implementation of the ONC information blocking rule.**

Detailed Comments

Individual Right of Access (45 CFR 164.524)

Strengthening the Access Right to Inspect and Obtain Copies of PHI

While MGMA supports the patient's right to inspect and obtain copies of their PHI in a designated record set, we are cautious about expanding this right to include the ability to take videos and photographs, particularly at the point of care. Similarly, MGMA is concerned with the proposed provision to be added to 45 CFR 164.524(c)(3), which would make it impermissible for a covered healthcare provider to delay the right to inspect when PHI is readily available at the point of care in conjunction with a healthcare appointment.

Such requests to take photos and videos at the point of care would likely result in unreasonable workflow disruptions for healthcare providers and take time away from other patient care due to scheduling limitations for the clinician. It would also require medical practices to develop and implement new policies and procedures to ensure that these additional access rights do not put the privacy of other patient records at risk. The civil monetary penalties associated with HIPAA

violations are costly, and practices will want to take extra precautions to ensure that they do not create scenarios in which patient data is compromised.

Additionally, as one member practice aptly pointed out, clinicians frequently initiate a visit note at the time of the patient encounter and later finalize it, often with substantive revisions. Typically, they are waiting for results of a diagnostic test or additional information to become available. If a patient takes a photo or video of a note at the point of care and subsequently sees something different in their record, it may create significant stress and confusion.

MGMA opposes a blanket mandate that medical practices always allow patients to take photographs and videos at the point of care without delay. Such a requirement is overly prescriptive and does not allow clinicians to use their professional judgement in deciding when it is or is not appropriate for the patient to photograph or record their medical record. This decision should be left up to the discretion of the treating clinician within the context of the patient-provider relationship.

Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access

The current HIPAA Privacy Rule permits a covered entity up to 30 days to respond to a patient access request and up to an additional 30-day extension with notice to the patient. These time periods for responding to patient record requests were established in an effort to be responsive to the patient while also being fair to the practice responsible for compiling the record. **MGMA opposes shortening this timeline in the current environment and urges OCR to maintain the existing 30-day response limit with the option for a 30-day extension when written notice is provided to the patient.**

As OCR has stated previously, the HIPAA Privacy Rule is intended to set the outer limit for providing access, not indicate the desired or best result. In the vast majority of instances, the patient does not require their designated record set immediately. Waiting even the full 30 days does not prove a hardship in most circumstances. In cases where PHI is required for clinical purposes, physicians and medical practices make every effort to expedite the retrieval of that information and provide it as quickly as possible to the patient or other care setting (often the same day it is requested). We note that shortening the timeline to 15 calendar days would create a *de facto* priority to meet every request as quickly as possible, which may prohibit practices from timely responding to requests that are actually urgent or emergent in nature.

Routine transfers of patient data, with no time requirements, are typically accomplished well within the permitted 30 days, but there are some legitimate circumstances on the practice side that would merit a longer timeframe to meet certain requests. MGMA enumerated in detail these circumstances in our response to OCR's 2018 RFI, including (but not limited to) situations in which:

- The requested PHI is maintained in multiple facilities,
- The requested PHI is maintained in multiple systems and/or in multiple formats,
- The request is in a different form/format than how it is stored, and there is a need to convert the stored format(s) into the one requested by the patient, and
- The clinician desires to review/redact portions of the record in cases where they believe the disclosure could be harmful to the patient or another individual.

While some individual access requests should be relatively easy to fulfill (e.g., those that can be satisfied through the use of Certified EHR Technology), the HIPAA Privacy Rule recognizes that there may be other circumstances where additional time and effort is necessary to locate and format the PHI that is the subject of the request. As medical groups continue to implement provisions of the ONC information blocking rule and upgrade their health information technology (IT) to incorporate standardized application programming interfaces (APIs), fulfilling such requests in a shorter timeframe will become more feasible. However, the provisions of the ONC rule span an implementation timeline through the end of 2022. Imposing this shortened timeframe at the present would unduly penalize practices that have not yet been able to upgrade their systems for any variety of reasons, including through no fault of their own (i.e., EHR vendor latency, third-party contractor delays, financial hardships, etc.).

Such a requirement to shorten the response time would also disproportionately and adversely affect smaller, independent medical practices. In general, these practices have a larger hurdle to climb in order to comply with the ONC information blocking rule given they do not have entire IT departments and designated staff to help with the implementation of new health IT, as do their counterparts that are owned or affiliated with hospitals and large health systems. One independent primary care practice expressed a concern with shortening this timeframe, given the difficulty they have had maintaining staff during the COVID-19 pandemic at the same time as they are struggling to catch up to comply with information blocking requirements. Additional changes in the present environment are simply too much for a small practice to handle at once, particularly in light of the staffing challenges they are already facing.

As an alternative to shortening the 30-day timeline to meet requests, MGMA agrees that there should be a process to prioritize urgent or other high priority access requests, as OCR has proposed. In many cases, practices already rely on such processes to meet urgent patient requests, particularly when they affect the provision of urgent or emergent medical care. However, there should not be a mandate that this process be written or followed in every circumstance. Should this proposal be finalized, we urge OCR to provide additional regulatory or subregulatory guidance to help covered entities understand how “urgent” and “high priority” requests should be defined and to create a model policy for prioritizing urgent or other high priority access requests. Covered entities should then be given the option to adopt a policy the same or similar to OCR’s model policy.

Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

MGMA supports OCR's goal of reducing barriers for patients seeking to have their electronic PHI shared with third parties of their choosing. However, we have significant concerns about OCR's proposal that a covered healthcare provider be required to respond to an individual's *oral* request to direct an electronic copy of PHI in an EHR to a third party when the request is "clear, conspicuous, and specific." Although an oral request may comply with this new standard for clarity and specificity, we are concerned about the unintended consequences of potential misunderstandings, miscommunications, disclosures to incorrect recipients. There is too much room for misinterpretation in this proposal, and the risk is too high for medical practices that may ultimately be held liable for a HIPAA violation in the absence of a request documented in writing.

Requests made electronically through a patient portal, however, are a desirable alternative to oral requests. These requests are more convenient for patients than current procedures that require hard copies of the disclosure request to be written, signed by the individual, and made in person. Electronic requests made in writing would also alleviate the trepidation medical practices have around acting upon oral requests with no written record of the interaction endorsed by the patient. **MGMA therefore urges OCR to avoid creating a mandate for healthcare providers to act upon oral requests to disclosure electronic PHI to third parties and instead provide the option for patients to make such requests electronically through patient-facing portals.**

Additionally, MGMA is concerned with the proposal establishing a new role for the medical practice to act as a "Requester-Recipient" on behalf of patients seeking medical records from other covered entities. Especially in the context of OCR's other proposals, this would create a significant administrative burden for the practice to triage all such patient requests to solicit and obtain medical records from all enumerated "Discloser" providers, particularly if the ability to make such requests can be made verbally and require action in a shorter timeframe.

Even if all previously discussed proposals are not finalized, this requirement would still result in a substantial increase in time and staffing required to fulfill such patient requests, particularly for smaller, independent practices and those that do not yet have a fully mature health IT infrastructure. The amount of burden this requirement would place on medical practices is difficult to quantify and likely different depending on practice size, patient demographics, specialty, and other factors. Ultimately, though, we fear this requirement would further delay other access requests and distract practice staff from more essential patient care activities.

Adjusting Permitted Fees for Access to PHI and ePHI

MGMA supports OCR's proposal to maintain the healthcare provider's ability to charge a fee in cases where the patient directs the transmission of an electronic copy of PHI in an EHR, or a non-electronic copy of PHI through means other than an internet-based method, to a third party.

However, in creating such a fee structure, OCR is overly prescriptive in how the fee should be calculated and underestimates the costs involved with meeting such a request.

In addition to labor, time, and supply costs factored into the proposed fee structure, medical practices also incur considerable costs to implement and maintain an EHR with API capabilities sufficient to meet new standards established by the ONC rule. These and other costs should reasonably be factored into the patient fee to more accurately represent the administrative and technological costs associated with maintaining and transferring patient records. Given the fact that these costs vary widely among medical groups by ownership structure, specialty, practice size, and other factors, it would be difficult to capture that cost in a predetermined fee structure. For this reason, OCR should not require that a specific cost-based fee structure be followed when providers receive requests to transmit PHI to a third party. OCR should assume that providers are acting in good faith to charge patients reasonable, cost-based fees in accordance with current HIPAA regulations and other state and local policies.

Moreover, MGMA is concerned with OCR's proposal to prohibit fees in cases where an individual uses an internet-based method to direct electronic copies of PHI in an EHR to any third party under the assumption that no cost would be incurred by the provider. We disagree with this assumption for the reasons outlined above. As previously discussed, patient medical information, even when stored electronically, often resides in multiple systems, and in many cases, the requested information must still be collected manually by practice staff. For this reason, a cost-based fee should still apply in cases where internet-based methods are used to transfer PHI to a third party. **If OCR decides to implement a cost-based fee structure, MGMA recommends that the fee structure recognizes the difference in cost when manual effort is required to meet a request, thereby better aligning with the fee structure established by ONC.**

Reducing Identity Verification Burden for Individuals Exercising the Right of Access (45 CFR 164.514(h))

MGMA supports the proposal to prohibit unreasonable identity verification measures on patients and their personal representatives in exercising their rights under the HIPAA Privacy Rule. We agree that verification measures should not pose an unnecessary obstacle for a patient seeking access to their PHI. However, as we expressed in our comments on the ONC information blocking rule, MGMA has significant concerns around sharing sensitive patient information with personal health applications not covered under HIPAA. It is imperative that OCR work together with ONC to develop an approach for how practices and other entities that are, for the most part, covered entities or business associates under HIPAA, share EHI with these non-HIPAA covered entities and ensure that such third-party applications are equipped to securely handle sensitive patient information.

We are concerned that patients will not have adequate information to be educated consumers and may not fully comprehend that they are assuming the risk of the security practices implemented

by their chosen personal health application. Consumers do not necessarily understand when their information is and is not protected by HIPAA. While we appreciate OCR's guidance clarifying that healthcare providers are not responsible under the HIPAA Security Rule for verifying the security of a patient's chosen third party application, this "safe harbor" does not address the potential vulnerability of patient information after it is sent to the application.

Further, we reiterate that ONC and OCR should engage with the private sector in the development of a privacy and security trust or certification framework for third-party applications seeking to connect to APIs of certified health IT. Once established, ONC should permit practices to limit the use of their APIs to third party applications that have agreed to abide by the framework. Such a program would not only foster innovation, but also establish improved assurance to patients around the security of their EHI.

Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations (45 CFR 164.506)

As with our concerns around the sharing of PHI with third-party personal health applications outlined above, MGMA is similarly concerned with the proposal to share PHI with social services agencies, community-based organizations, home- and community-based service providers, and other similar third parties that provide health-related services to individuals. These types of organizations are not governed by HIPAA, and there is no way for healthcare providers to know what types of privacy safeguards they have in place to protect sensitive patient information.

We are also reluctant to allow patient PHI to freely flow to these organizations without a patient's express authorization or consent. There need to be significant guardrails in place to ensure that only the appropriate amount of data is shared with the correct organization and with explicit patient consent (to the extent that is possible in non-emergent situations). **In conjunction with the information blocking regulations that make the sharing of patient data compulsory upon request, MGMA has significant concerns with this proposal due to the lack of legal and regulatory safeguards in place to protect the privacy and security of sensitive health information once it is shared with a non-HIPAA covered entity.**

Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances (45 CFR 164.502 and 164.510–514)

MGMA supports OCR's proposal to amend five provisions of the HIPAA Privacy Rule to replace the "professional judgment" standard with the "good faith belief" standard under which covered entities would be permitted to make certain uses and disclosures in the best interests of individuals experiencing substance use disorder (SUD), serious mental illness (SMI), and in emergency circumstances. We believe that this change in standard would allow other appropriate

and trusted non-physician practice leaders to act in a SUD or SMI patient's best interests without waiting on the approval of a physician.

While a physician's clinical context and training may at times be necessary or desirable, we believe the current professional judgement standard may create a bottleneck and delay appropriate care for patients in distress. Therefore, MGMA believes that the creation of this new standard will improve outcomes and access to timely care overall. If finalized, we recommend that OCR issue additional subregulatory guidance to help medical practices operationalize these changes and provide clear guidance around which non-clinical care personnel would be authorized to act in good faith with examples of permissible actions and scenarios.

Eliminating Notice of Privacy Practices Requirements Related to Obtaining Written Acknowledgment of Receipt, Establishing an Individual Right to Discuss the NPP With a Designated Person, Modifying the NPP Content Requirements, and Adding an Optional Element (45 CFR 164.520)

MGMA supports the proposal to eliminate the requirement for a covered healthcare provider with a direct treatment relationship with an individual to obtain a written acknowledgement of the receipt of the NPP. There is no practical use of the acknowledgement of receipt of the NPP or documentation of the good faith efforts made by the practice at securing an acknowledgment. These forms are almost never reviewed by the patient once collected, and few if any patients ever ask to review or modify these forms. Furthermore, patients and providers alike often misunderstand the purpose of the NPP due to its often-confusing language. Removing the written acknowledgement requirement and the six-year retention requirement would be a welcome reduction in unnecessary administrative burden on medical groups.

To the extent that a change to the content requirements of the NPP is necessary to remove the written acknowledgement requirement, MGMA is supportive of this proposal. We also view this content revision as an opportunity to help patients and providers better understand what the NPP is and is not. However, there is administrative burden inherent in making the enumerated content changes to the NPP and updating it in all the physical and electronic places in which it currently resides. It is common for practices to engage with legal counsel in the development of their NPP, and it would be necessary for them to reengage such counsel in order to revise the NPP to comply with new content standards. We encourage OCR to ensure medical practices have sufficient time to meet the new NPP content requirements if finalized.

Currently, OCR's model NPP is a helpful baseline for medical practices in that it is well-constructed and patient focused. MGMA recommends that OCR update its model NPP to sufficiently capture the various revisions it has proposed and thereby easily enable medical groups to adapt the model for their own use. Ideally, this adoption of a model NPP would require as little burden on the practice as possible and minimal reliance on their own legal counsel. If OCR finalizes this proposal, MGMA recommends that OCR engage with consumer-facing and physician practice organizations to promote the use of the OCR model NPP.

Finally, we emphasize that education is critical if patients are to be made aware of their rights under HIPAA. In many cases, patients rely on their treating provider and provider's medical practice to provide this education. We do not believe that the onus should be on the provider and medical practice to make patients aware of their rights under HIPAA. MGMA urges OCR to be more proactive in conducting consumer outreach to facilitate patient education on this topic.

Conclusion

MGMA appreciates the opportunity to provide recommendations to OCR on ways to modify the HIPAA Privacy Rule without compromising the security of patient data or imposing undue administrative burdens on medical groups during an already challenging time. As the voice of the country's medical groups, MGMA is committed to engaging with OCR going forward to inform efforts to promote patient access to their health information and remove unnecessary barriers to care coordination and case management. We are pleased to be able to offer our assistance and feedback now and in the future. Should you have any questions regarding these comments, please contact Matt Devino at mdevino@mgma.org or 202.293.3450.

Sincerely,

/s/

Anders Gilberg, MGA
Senior Vice President, Government Affairs