Medical Group Management Association®

February 12, 2019

Roger Severino, JD
Director
Office for Civil Rights
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

RE: Request for Information on Modifying HIPAA Rules To Improve Coordinated Care

Dear Director Severino:

The Medical Group Management Association (MGMA) is pleased to submit the following comments in response to the request for information entitled, "Request for Information on Modifying HIPAA Rules To Improve Coordinated Care," published on Dec. 14, 2018. We believe modification of the current HIPAA requirements have the potential of significantly improving the ability of physician practices to facilitate efficient care coordination and promote the transformation to value-based healthcare. At the same time, we caution the Office for Civil Rights (OCR) not to proceed with initiatives that create additional administrative burden on practices with little or no benefit to the patient.

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 45,000 medical practice administrators, executives, and leaders, MGMA represents more than 12,500 organizations of all sizes, types, structures and specialties that deliver almost half of the healthcare in the United States.

An increasing number of physician practices are acquiring certified health IT and leveraging technology to improve care coordination for their patients and to participate in value-based care arrangements. The deployment of effective federal policies that assist practices in those endeavors is critical if practices are to take full advantage of their EHRs and patients are to reap the benefits of streamlined sharing of clinical data. The HIPAA Privacy and Security Rules laid out a framework to ensure that protected health information (PHI) would be kept confidential and secure. These rules, however, were finalized (HIPAA Privacy 2003, HIPAA Security 2005) prior to the widespread use of EHRs in physician practices and prior to the advancement of value-based care arrangements. Certain provisions of these rules now can act as impediments to the efficient communication of PHI.

MGMA supports the efforts of OCR to identify and modify those provisions which serve as roadblocks to PHI movement. In this RFI, OCR lays out a number of critical issues with the HIPAA Privacy rule and asks a series of questions. We appreciate the opportunity to provide input on these critical issues and urge the agency to fully engage impacted stakeholders, including physician practices, patient advocates, EHR software vendors, and other critical stakeholders, in a formal outreach process prior to release of the next iteration of the regulation. The goal of this outreach should be to ensure that any future regulation appropriately balances the need to

adequately protect PHI and provide patients access to the information they need while not overly burdening physician practices and their business associates.

Summary of Key Recommendations

MGMA supports OCR's efforts to modify the HIPAA Privacy and Security Rules to allow practices to receive and transmit patient data more efficiently in support of patient care delivery. MGMA highlights the following high-level recommendations to ensure that OCR ultimately meets the needs of practices and the patients they serve:

1. **First do no harm**. Any modifications to the HIPAA Rules should not impose additional administrative burdens on physician practices. In fact, modifications should reduce barriers to care coordination, case management, and value-based care.

2. **Do not move forward with accounting of disclosures for treatment, payment, and healthcare operations (TPO).** Accounting for TPO disclosures would be excessively burdensome and unnecessary. MGMA surveys show that very few patients are asking for these reports, and current EHR technology cannot produce these reports.

3. **Do not require paper records and oral communications in an accounting of disclosures report.** While reporting on electronic TPO disclosures itself would extremely challenging, reporting on disclosures made on paper and by practice clinical and administrative staff orally would be next to impossible.

4. **Maintain the current response times for practices to respond to patient requests for a copy of their PHI.** Currently, practices have up to 30 days to provide the patient their PHI (with the potential of a one-time 30-day extension). As there is tremendous variation in practice technology, medical record formats, and location of medical records, this maximum time is necessary.

5. **Remove the requirement for practices to obtain or make a "good faith effort" to obtain written acknowledgement of the Notice of Privacy Practices (NPP).** Obtaining the written acknowledgement of the NPP or making a good faith effort to obtain it is an unnecessary burden on practices and of little value to the patient. Less burdensome options for sharing the NPP with patients should be allowed.

6. **Do not move forward with a mandate requiring a covered provider to disclose PHI to business associates or another covered entity.** Clinicians should be permitted to use their professional judgement and determine when it is necessary and appropriate to disclose a patient's health information.

7. **In the case of ransomware attacks, educate clinicians, don't penalize them.** OCR should not "blame the victim" by considering a ransomware attack an automatic data breach. Rather, the agency should seek to leverage the collective intelligence from these attacks to educate physician practices on how to prevent them from happening and what steps to take should they experience a cyberattack.

8. **Enhance education for both patients and physician practices.** A better understanding of the regulations will assist both communities in better understanding their rights and obligations.

DETAILED RFI COMMENTS

SECTION A

Promoting Information Sharing for Treatment and Care Coordination

OCR Questions

- *How long does it take for covered entities to provide an individual with a copy of their PHI when requested pursuant to the individual's right of access at 45 CFR 164.524?*
- *How long does it take for covered entities to provide other covered entities copies of records that are not requested pursuant to the individual's right of access?*
- *Does the length of time vary based on whether records are maintained electronically or in another form (e.g., paper)?*
- *For instance, do some types of health care providers or plans take longer to respond to requests than others?*
- *How feasible is it for covered entities to provide PHI when requested by the individual pursuant to the right of access more rapidly than currently required under the rules?*
- *What is the most appropriate general timeframe for responses?*
- *Should any specific purposes or types of access requests by patients be required to have shorter response times?*
- *Should covered entities be required to provide copies of PHI maintained in an electronic record more rapidly than records maintained in other media when responding to an individual's request for access? If so, what timeframes would be appropriate?*
- *What burdens would a shortened timeframe for responding to access requests place on covered entities? OCR requests specific examples and cost estimates, where available.*

MGMA Response

Current law permits a practice up to 30 days to produce the requested record pursuant to a patient's request, and up to an additional 30 days with notice to the patient. These time periods for responding to patient record requests was established in an effort to be responsive to the patient while also being fair to the practice responsible for compiling the record.

There are multiple reasons why a practice may require additional time to produce a medical record for a patient:

- PHI maintained in multiple facilities. Practices may have multiple facilities, each potentially maintaining separate medical records for a patient. Compiling the full record set from these various facilities will require considerable staff time and coordination.

- PHI maintained in multiple systems and in multiple formats. In many practices, PHI is maintained electronically in multiple systems. While the bulk of the PHI could be housed in the main EHR, other parts of the record could be in other clinical or administrative systems. For example, if the practice conducts clinical trials, it may capture and store the clinical data associated with the trial in a separate file from the traditional medical record. A practice may have PHI contained in a system designed to benchmark non-deidentified quality data, while others may have electronic data stored in systems that are strictly performing revenue cycle functions. Additional time would be required by staff to compile the complete designated record set to fulfill a patient request.

  Even if a practice has migrated to an EHR, it is likely that they have not scanned in every patient record. Many EHRs, for example, contain only the last few years of patient records. Older paper records are typically kept either in a designated area of the practice or stored offsite. However, these older records would be considered part of the designated record

set and would need to be included in a complete medical record as requested by a patient. Assembling these records would require considerable staff time.

- Form and format. Patients have the right to request the practice provide the designated record set in a specific form and format. For example, the patient may request their designated record set be provided to them in PDF and stored on a USB "thumb" drive. With the record potentially being in multiple formats (i.e., PDF, Excel, images, paper), it will take staff additional time to convert these multiple formats into the one requested by the patient.

- Physician review of the record. Current HIPAA regulations permit the clinician to review the medical record prior to it being provided to the patient. Clinicians have the right to redact portions of the record should they believe disclosure of that information could be harmful to either the patient or another individual. This process requires sufficient time to both compile the complete record and have the appropriate review take place.

OCR recognizes that 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.

We agree with OCR that the Privacy Rule is intended to set the outer time limit for providing access, not indicate the desired or best result. In the vast majority of instances today, the patient does not require their designated record set immediately and waiting even the full 30 days does not prove a hardship on the patient. In cases where PHI is required for clinical purposes (i.e., referrals, coordination of care, transfer of care), physician 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).

MGMA recommends OCR adopt the following patient access policies:

- Maintain the current approach of providing the practice up to 30 days to fulfill the patient request for access to their medical record.

- Maintain the current approach of providing a one-time additional 30-day extension, with written notice of the extension provided to the patient.

- Maintain the current approach of permitting the clinician to review the designated record set and to redact any information that could prove harmful to either the patient or someone else prior to it being provided to the patient.

- Engage in an educational campaign aimed at informing patients of the rights under HIPAA to access their medical record (or a specific component of the record) and that they can request that it be provided to them in a specific time frame and format. This campaign could emphasize that practices should provide the record as quickly as possible and discuss the request with the patient to determine if they want the entire medical record or just specific information contained in the record.

- Many practices now employ a patient portal that permits the patient to retrieve significant portions of their designated record set. While the portal may not capture, for example, older records created prior to the practice adopting its EHR, it will typically have the information needed by the patient, such as recent lab results, medications, allergies, etc. Retrieving the complete record set, beyond what is captured in the patient portal, will take

additional time for practice staff.

For the components of the designated record set contained in the patient portal, the information should be available to the patient within 7 business days of the information being produced by the practice. This approach would closely mirror the Patient Electronic Access requirement of the 2019 Meaningful Use program—providing patients the ability to view online, download, and transmit their health information within 2 business days of the information being available to the eligible professional. The 5 additional days would assist those practices who have patient portals but who do not use 2015 Edition CEHRT.

Clearinghouse activities

OCR Questions

- *How commonly do business associate agreements prevent clearinghouses from providing PHI directly to individuals?*
- *Should health care clearinghouses be subject to the individual access requirements, thereby requiring health care clearinghouses to provide individuals with access to their PHI in a designated record set upon request? Should any limitations apply to this requirement? For example, should health care clearinghouses remain bound by business associate agreements with covered entities that do not permit disclosures of PHI directly to an individual who is the subject of the PHI?*
- *Alternatively, should health care clearinghouses be treated only as covered entities—i.e., be subject to all requirements and prohibitions in the HIPAA Rules concerning the use and disclosure of PHI and the rights of individuals in the same way as other covered entities—and not be considered business associates, or need a business associate agreement with a covered entity, even when performing activities for, or on behalf of, other covered entities? Would this change raise concerns for other covered entities about their inability to limit uses and disclosures of PHI by health care clearinghouses? For example, would this change prevent covered entities from providing assurances to individuals about how their PHI will be used and disclosed? Or would covered entities be able to adequately fulfill individuals' expectations about uses and disclosures through normal contract negotiations with health care clearinghouses, without the need for a HIPAA business associate agreement? Would covered entities be able to impose other contractual limitations on the uses and disclosures of PHI by the health care clearinghouse?*
- *If health care clearinghouses are not required to enter into business associate agreements with the other covered entities for whom they perform business associate functions, should such requirement also be eliminated for other covered entities when they perform business associate functions for other covered entities*

MGMA Response

MGMA believes healthcare clearinghouses should be subject to the individual access requirements as other covered entities, but that they should be bound by any business associate agreement they sign with another covered entity. While patients do have the right to access information themselves from any HIPAA-covered entity, clearinghouses perform a very different role than providers or health plans and as such, patients may not have the same need to access PHI from them.

Clearinghouses should be bound by the business associate agreements with covered entities that do not permit disclosures of PHI directly to an individual who is the subject of the PHI.. The

practice is in the best position to review a patient's medical record request and supply them with the information they need.

Further, in the RFI (Vol. 83, No. 240, p. 64304), OCR states, "*Nevertheless, the PHI that clearinghouses possess could provide useful information to individuals. For example, clearinghouses may maintain PHI from a variety of health care providers, which may help individuals obtain their full treatment histories without having to separately request PHI from each health care provider."*

We do not believe this characterization of clearinghouses is completely accurate. Clearinghouses typically perform the role of converting non-standard healthcare transactions to standard transactions from one covered entity (most likely a provider) to either another clearinghouse designated by a health plan, or to the health plan itself. The patient's PHI is not created by the clearinghouse but rather created by the provider or health plan and transmitted by the clearinghouse. Any PHI disclosed by the practice to the clearinghouse would be done for purposes of a specific transaction. For example, a provider may disclose to the clearinghouse a specific component of the medical record to transmit to the health plan in support of a claim submission or prior authorization request.

We are also concerned that modifying this provision could eliminate the requirement for practices to enter into business associate agreements with clearinghouses, and even potentially invalidating existing agreements between practices and clearinghouses. We agree that business associates should be permitted to respond directly to individuals' access requests and provide individuals with access to an aggregate view of the PHI maintained by them. However, we oppose any OCR policy that would reverse or invalidate existing contract terms between practices and clearinghouses.

Barriers to obtaining PHI

OCR Questions

- *Do health care providers currently face barriers or delays when attempting to obtain PHI from covered entities for treatment purposes?*
- *Do covered entities ever affirmatively refuse or otherwise fail to share PHI for treatment purposes, require the requesting provider to fill out paperwork not required by the HIPAA Rules to complete the disclosure (e.g., a form representing that the requester is a covered health care provider and is treating the individual about whom the request is made, etc.), or unreasonably delay sharing PHI for treatment purposes?*

MGMA Response

It is common for a practice (or patient at the request of the practice) requesting medical records for treatment purposes to encounter challenges in receiving that information. These challenges are most often due to a lack of education of administrative staff regarding what is considered a permissible disclosure and fear from staff that an incorrect disclosure decision could lead to an enforcement action against their practice. This fear has been exacerbated by the public announcements of OCR enforcement activity and the heavy monetary fines lodged against practices and other covered entities for data breaches. Some organizations have adopted policies of refusing to release patient records, even for TPO purposes, without a signed patient authorization. These issues could be addressed, at least in part, by OCR undertaking an education and communication strategy aimed at informing patients and covered entities of the right of the practice to disclose PHI for TPO purposes.

HIPAA has long recognized the seamless sharing of information for TPO is essential for the efficient and safe delivery of patient care. This information sharing becomes even more critical in a value-based care environment.

Disclosing PHI

OCR Questions

- *Should covered entities be required to disclose PHI when requested by another covered entity for treatment purposes?*
- *Should the requirement extend to disclosures made for payment and/or health care operations purposes generally, or, alternatively, only for specific payment or health care operations purposes?*
- *Would this requirement improve care coordination and/or case management? Would it create unintended burdens for covered entities or individuals? For example, would such a provision require covered entities to establish new procedures to ensure that such requests were managed and fulfilled pursuant to the new regulatory provision and, thus, impose new administrative costs on covered entities? Or would the only new administrative costs arise because covered entities would have to manage and fulfill requests for PHI that previously would not have been fulfilled?*
- *Should any limitation be placed on this requirement? For instance, should disclosures for healthcare operations be treated differently than disclosures for treatment or payment? Or should this requirement only apply to certain limited payment or health care operations purposes? If so, why?*
- *Should business associates be subject to the disclosure requirement?*

MGMA Response

As discussed above, practices may be reluctant to disclose medical records to the patient's family, their caregivers, or other providers involved in the care of the patient if that would potentially be against the wishes of the patient. We recommend OCR develop clear guidance regarding what PHI is permitted to be disclosed, when it is permitted to be disclosed, and to whom it can be disclosed.

MGMA opposes any mandate or requirement for a covered provider to disclose PHI to another covered entity for any purpose. Requiring practices to share information that could be in opposition to the wishes or stipulations of a patient could supersede medical decision-making and clearly removes the right of the patient to control who has access to their health information. We are also concerned that forcing practices to disclose PHI greatly increases the chance that an inappropriate disclosure will take place. In particular, requiring practices to disclose PHI for purposes other than treatment raises the specter of cyberattacks and other malicious acts where PHI is disclosed by the practice in good faith, yet the patient's information is stolen. Mandating this disclosure requirement on practices would be counter to the federal government's clear efforts at combating identity and medical record theft. Imposing this type of disclosure requirement would also place the clinician in the difficult position of attempting to decide which harm would be worse--not releasing the information that could be used in the treatment of the patient or risking an inappropriate disclosure.

OCR Question

- *Should any of the above proposed requirements to disclose PHI apply to all covered entities (i.e., covered health care providers, health plans, and health care clearinghouses), or only a subset of covered entities? If so, which entities and why?*

MGMA Response

As we state above, while a covered provider should be encouraged to disclose PHI to another covered entity when appropriate, they should be permitted to exercise their professional judgement and not be mandated to disclose the patient's PHI.

OCR Questions

- *Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to any of the matters discussed in Questions 7 and 8?*
- *Would such a requirement create any unintended adverse consequences? For example, would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester?*
- *Do the risks associated with disclosing PHI to health care providers not subject to HIPAA's privacy and security protections outweigh the benefit of sharing PHI among all of an individual's health care providers?*

MGMA Response

As we discussed above, practices that are covered entities should not be mandated to disclose PHI to non-covered healthcare providers. As these non-covered entities are not required to comply with the existing HIPAA regulations, there would be no guarantee that the PHI disclosed would be sufficiently protected. In this environment, we would expect that practices would seek to get contractual reassurance that the recipient of the PHI met a minimum level of security. The development and deployment of these additional policies would, of course, add to the administrative burden faced by practices and potentially increase their liability. Should OCR move forward with this regulatory modification, the agency should create a safe harbor for practices to ensure that their good faith efforts to comply with the requirement does not expose them to OCR enforcement or state law privacy requirements should there be an inappropriate disclosure.

Non-covered and covered entities

OCR Questions

- *Should a non-covered health care provider requesting PHI from a HIPAA covered entity provide a verbal or written assurance that the request is for an accepted purpose (e.g., TPO) before a potential disclosure requirement applies to the covered entity receiving the request? If so, what type of assurance would provide the most protection to individuals without imposing undue burdens on covered entities?*
- *How much would it cost covered entities to comply with this requirement? Please provide specific cost estimates where available.*

MGMA Response

While receiving verbal or written reassurance from a non-covered entity that the request for PHI is for TPO purposes could be helpful, this may not be sufficient to reduce risk. Practices are concerned that they would be held liable should their release of PHI result in a data breach or other form of inappropriate disclosure. To reiterate, should OCR move forward with this regulatory modification, the agency must create a safe harbor for practices to ensure that their good faith efforts to comply with the requirement does not expose them to OCR enforcement or state law privacy requirements.

OCR Questions

- *Should OCR create exceptions or limitations to a requirement for covered entities to disclose PHI to other health care providers (or other covered entities) upon request? For example, should the requirement be limited to PHI in a designated record set?*
- *Should psychotherapy notes or other specific types of PHI (such as genetic information) be excluded from the disclosure requirement unless expressly authorized by the individual?*

MGMA Response

We oppose any effort to mandate that covered providers disclose PHI. Clinicians must be permitted to use their best professional judgement in determining what PHI should be disclosed to other covered providers upon request. In making this determination, clinicians will take into account the best interests of the individual patient. In particular, extremely sensitive PHI requires additional consideration prior to disclosure, including psychotherapy notes, HIV status, genetic information and other types of PHI. Requiring clinicians to disclosure this type of information without the patient's consent and contrary to the professional judgement of the clinician could be harmful to the patient.

Timeliness of disclosure

OCR Questions

- *What timeliness requirement should be imposed on covered entities to disclose PHI that another covered entity requests for TPO purposes, or a non-covered health care provider requests for treatment or payment purposes?*
- *Should all covered entities be subject to the same timeliness requirement? For instance, should covered providers be required to disclose PHI to other covered providers within 30 days of receiving a request?*
- *Should covered providers and health plans be required to disclose PHI to each other within 30 days of receiving a request?*
- *Is there a more appropriate timeframe in which covered entities should disclose PHI for TPO purposes?*
- *Should electronic records and records in other media forms (e.g., paper) be subject to the same timeliness requirement?*
- *Should the same timeliness requirements apply to disclosures to non-covered health care providers when PHI is sought for the treatment or payment purposes of such health care providers?*

MGMA Response

We would urge OCR to develop a policy for the timeliness of practices to release PHI to another covered entity that mirrors the current policy for release of PHI to patients. The Privacy Rule is intended to set the outer time limit for providing access, not indicate the desired or best result. Just as in the case with release of PHI to patients today, in the majority of cases the covered entity requesting the PHI will not need to wait the full 30 days before receiving the patient information. Due to the collaborative nature of clinicians and their desire to provide the best possible care for their patients, cases where the transfer of information is critical to the care of the patient are expedited. Routine transfers of patient data, with no time requirements, are still typically accomplished well within the permitted 30 days. As part of its enhanced education effort, OCR could emphasize the importance of this information transfer and encourage expedited handling of these patient information requests.

OCR Questions

- *Should individuals have a right to prevent certain disclosures of PHI that otherwise would be required for disclosure? For example, should an individual be able to restrict or "opt out" of certain types of required disclosures, such as for health care operations?*
- *Should any conditions apply to limit an individual's ability to opt out of required disclosures? For example, should a requirement to disclose PHI for treatment purposes override an individual's request to restrict disclosures to which a covered entity previously agreed?*

MGMA Response

Patients currently have considerable "opt out" options regarding their health information when obtaining care at a physician practice. Should they have concerns with individuals in the practice who have access to their medical record, they have the right to request that a specific staff member not be permitted to access their record. They also have the right to ask the practice not to submit a claim to their insurance for a service or test, providing they pay for that service or test in full out-of-pocket. And finally, patients concerned about who can access their health record have the right to opt out completely from receiving care from the practice by going to another care setting or by foregoing care entirely.

Should the patient have the right to opt out from practice PHI disclosures for treatment purposes, it would put the practice in an extremely difficult situation. Sharing PHI within the practice is a critical component of the care delivery process. In particular, nurses and physicians share information continually, but more generally, information is shared throughout the practice's clinical and administrative teams. Being prohibited from these disclosures would significantly impede the ability of practice staff to render care and fully document encounters, and practices might refuse to treat a patient under these conditions.

Similarly, permitting patients to opt out of disclosures made for purposes of healthcare operations would impose a significant and unnecessary administrative burden on the practice. Attempting to segment the medical record by which data could or could not be used for administrative purposes such as benchmarking and quality reporting is beyond the capabilities of most current EHRs and would require onerous manual segmenting of the medical record. If a patient has a specific concern regarding the use of their information, such as not wanting it to be used for fundraising purposes, it is likely the practice would comply with that request.

Additionally, if a patient opts out of disclosures for the purpose of healthcare operations, such a restriction on information sharing can potentially impede value-based activities within a network of physicians, such as performance evaluation, case management, quality assessment activities, care coordination activities, efforts to control total cost of care, and population-based healthcare improvement. For instance, by OCR's own example of a permitted disclosure for healthcare operations, an Accountable Care Organization's (ACO's) quality committee may exchange PHI to evaluate treatment and health outcomes of a patient that experienced a hospital-acquired infection for purposes of improving future outcomes. Such a restriction could also impede CMS' ability to provide feedback to group practices participating in quality reporting initiatives or a Medicare alternative payment model if the feedback involves beneficiary-identifiable claims data.

Under the Medicare Shared Savings Program, ACOs may request certain beneficiary-level claims data for patients that are candidates for assignment to aid in efforts to better coordinate care and implement individual, targeted care strategies. CMS determined this disclosure is permissible under HIPAA for healthcare operations when certain conditions are met. Despite having the legal authority to make such disclosures without providing patient notice, CMS requires ACOs to provide patients the opportunity to opt-out of data sharing. This has resulted in unnecessary confusion and burden, including that ACOs must track and maintain opt-out information.

Moreover, when a beneficiary declines to share data, the ACO is still held financially accountable for the beneficiary's cost of care, despite having restricted access to their information. CMS should expand, not restrict, the availability of beneficiary data to encourage ACOs to influence care management for all beneficiaries. Creating a patchwork of limitations on PHI disclosure not only increases physician practice burden but could potentially counteract care coordination efforts.

Due to the challenges associated with these types of potential opt out options, we would oppose expanding the current opt out options for patients and recommend that OCR encourage practices to comply with reasonable patient requests to limit or restrict disclosures.

Sharing PHI between providers

OCR Question

- *How would a general requirement for covered health care providers (or all covered entities) to share PHI when requested by another covered health care provider (or other covered entity) interact with other laws, such as 42 CFR Part 2 or state laws that restrict the sharing of information?*

MGMA Response

Clinicians will share PHI when it is in the best interests of the patient and complies with appropriate federal and state laws. Currently, 42 C.F.R. Part 2, for example, prohibits certain disclosures related to substance abuse treatment. Until this law is changed, clinicians will continue to abide by its provisions. We would strongly oppose any attempt by OCR to mandate clinicians to disclose PHI when requested by another covered healthcare provider. Clinicians must be able to use their professional judgement when disclosing PHI. There would be significant liability concerns associated with a PHI disclosure when the sending clinician knew that the disclosure was unlawful yet had to comply with the request due to this modification of the HIPAA Rule.

Information blocking

OCR Question

- *What considerations should OCR take into account to ensure that a potential Privacy Rule requirement to disclose PHI is consistent with rulemaking by the Office of the National Coordinator for Health Information Technology (ONC) to prohibit "information blocking," as defined by the 21st Century Cures Act?*

MGMA Response

We anticipate that the Office of the National Coordinator for Health Information Technology (ONC) will release regulations pertaining to data "blocking" in the near future. ONC is expected to outline situations where clinicians are required to share patient PHI and situations where it is appropriate for the clinician to withhold PHI from a requesting entity. We urge OCR to refrain from any modifications to HIPAA in this policy area prior to finalization of this ONC rule.

Minimum necessary standard exceptions

OCR Questions

- *Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard? For instance, should population-based case management and care coordination activities,*

claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development be excepted from the minimum necessary requirement?

- *Would these exceptions promote care coordination and/or case management? If so, how?*
- *Are there additional exceptions to the minimum necessary standard that OCR should consider?*

MGMA Response

We assert that the applicability of the minimum necessary standard to case management and care coordination disclosures should not pose a barrier when practices and their business associates are exercising good faith. Any perceived barriers created by the minimum necessary rule could be alleviated through guidance and education rather than a regulatory change. OCR, for example, could issue additional guidance on conditions where it is permissible despite the minimum necessary requirement to provide a practice and business associates with access to PHI for case management and care coordination purposes (in other words, where full access is the minimum necessary).

Additionally, an ACO may require access to the entire record set of each of its attributed patients to efficiently conduct case management or care coordination. Current OCR guidance on using and disclosing entire record sets indicates that the minimum necessary standard would not prevent such access. We encourage the agency to supplement this guidance by providing specific case management and care coordination examples.

Other federal laws could also prevent a practice from providing the entire record set for case management or care coordination purposes. As an example, 42 C.F.R. Part 2 requires substance use disorder treatment programs and persons or entities that receive information from such programs to obtain a specific consent from the individual before they can use or disclose the protected substance use disorder treatment information for case management or care coordination. Although the Substance Abuse and Mental Health Services Administration has made some modifications to the 42 C.F.R. Part 2, this agency has specifically excluded case management disclosures from this new pathway. As a result, covered entities may need to exclude information protected by 42 C.F.R. Part 2 from case management or care coordination disclosures even if such information would normally be considered part of the "minimum necessary" information to perform such services.

Condition-specific laws such as 42 C.F.R. Part 2 could create a greater barrier for case management and care coordination by the ACO than the minimum necessary rule. This reiterates the need for greater alignment between HIPAA and other federal and state laws governing the use and disclosure of medical records.

Public outreach and education

OCR Question

- *Would increased public outreach and education on existing provisions of the HIPAA Privacy Rule that permit uses and disclosures of PHI for care coordination and/or case management, without regulatory change, be sufficient to effectively facilitate these activities? If so, what form should such outreach and education take and to what audience(s) should it be directed?*

MGMA Response

As we state throughout this document, we believe enhanced patient and practice education will lead to significant improvement in the ability of the patient and the practice to understand their

rights and responsibilities under the law. Many of the challenges associated with data "blocking" and failure to have the PHI necessary for care coordination or case management can be traced back to an unfamiliarity with the law or misinterpretation of regulations. We recommend the following approaches to education be adopted by OCR:

- Partner with professional trade associations like MGMA in the development and implementation of online and face-to-face education aimed at physician practices.

- Partner with patient advocacy groups in the development and implementation of online and face-to-face education aimed at patients.

- Develop educational materials for posting on the OCR website to assist relevant stakeholder group better understand their rights and responsibilities. Included in these materials should be the application of key regulatory provisions to cases studies and a wide variety of clinical and administrative scenarios.

Care coordination provisions

OCR Questions

- *Are there provisions of the HIPAA Rules that work well, generally or in specific circumstances, to facilitate care coordination and/or case management? If so, please provide information about how such provisions facilitate care coordination and/or case management.*
- *In addition, could the aspects of these provisions that facilitate such activities be applied to provisions that are not working as well?*

MGMA Response

Physician practices are generally well aware of the requirements of the HIPAA Privacy and Security Rules. Under HIPAA, disclosures made for treatment purposes do not require patient authorization. Similarly, the minimum necessary provision of HIPAA permits the covered entity disclosing the PHI to rely on another covered entity only asking for the minimum necessary to perform a specific task. In the case of case management or care coordination, these two HIPAA provisions provide for the appropriate disclosure of the PHI at the time it is needed. Further, these provisions permit clinicians to use their best judgement regarding when to disclose PHI in the treatment of a patient. Clinicians are bound by comprehensive ethics requirements and as such are very reluctant to risk an inappropriate disclosure of PHI.

When seeking to modify the current HIPAA Rules, we recommend OCR follow a similar approach to the one described above and allow clinicians to apply their professional judgement in cases where PHI is required to move from their practice to another (appropriate) care setting or entity in support of case management or care coordination.

SECTION B

Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness

OCR Questions

- *What changes can be made to the Privacy Rule to help address the opioid epidemic? What risks are associated with these changes? For example, is there concern that*

encouraging more sharing of PHI in these circumstances may discourage individuals from seeking needed health care services?

- *Also is there concern that encouraging more sharing of PHI may interfere with individuals' ability to direct and manage their own care?*
- *How should OCR balance the risk and the benefit?*

MGMA Response

The nation is facing a critical challenge with the opioid epidemic, and there are many opportunities to help address this challenge. However, we do not believe that modifying the current HIPAA Privacy and Security Rules will significantly impact this crisis. Conversely, we do believe that educating patients and practices on issues regarding appropriate disclosures of PHI will have an impact.

Many believe that HIPAA is crafted to prevent clinicians from exchanging information with family members or caregivers of patients suffering from an opioid-related illness. We do not believe this to be the case. There is significant flexibility built into the regulations to permit clinicians to directly engage with those closest to the patient and those who can provide key data to assist the clinician in delivering the care needed.

Providing unfettered access to information must always be balanced with the wishes of the patient. We discourage OCR from pursuing changes to the HIPAA Privacy Rule that would result in patients suffering from opioid-related illnesses losing control over their medical record. These patients, if they are to confide in and trust their clinician, must still have the reassurance that their record will not be disclosed inappropriately.

SECTION C

Accounting of Disclosures

OCR Question

- *How many requests for an accounting of disclosures do covered entities receive annually and from what percentage of total patients? Of these, how many requests specify a particular preferred electronic form or format, and to what extent do covered entities provide the accounting in the requested form or format?*

MGMA Response

Patients having access to their health information is clearly one of the cornerstones of today's health system. Physician practices typically provide a wide variety of PHI to patients when they request it. This is most often requested when patients are (a) seeing another provider through a referral from the original provider, (b) switching providers, (c) compiling their own copy of their medical record, or (d) creating/maintaining a personal health record. Accounting of disclosures reports, however, are rarely requested, and when they are, they are typically requested for the purpose of (a) ascertaining who the practice has disclosed the non-TPO PHI to or (b) ascertaining who the practice has disclosed all PHI to (although in most cases, the practice does not compile and maintain non-TPO PHI disclosures and thus cannot fulfill the patient's request).

Under the HIPAA Privacy Rule, individuals have the right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date of the request. However, that right does not extend to several types of disclosures, including disclosures for TPO. The primary purpose for that exclusion is because disclosures for TPO are necessary for the day-to-day operation of a covered entity and occur in great numbers, so tracking them would be unduly burdensome on a covered entity.

HITECH changes the accounting of disclosures requirement to include even disclosures for TPO. Under HITECH, if a covered entity, such as a physician practice, utilizes an EHR, the organization will be required to account for TPO disclosures. Upon receiving a request for such a disclosure, the physician practice will be required to provide individuals with an accounting of disclosures of PHI which occurred within the 3 years prior to the date of the request. While HITECH requires the Secretary of the Department of Health and Human Services (HHS) to adopt regulations that take into consideration the individual's interest in knowing how PHI is used and disclosed, the legislation also directs the Secretary to determine the administrative burdens to covered entities in providing the accounting.

The fact that HITECH stipulates that the TPO accounting is only required for those physician practices that have adopted an EHR suggests that the government believes TPO disclosures would be collected and stored on this one clinical system. This is simply not the case. The majority of physician practices store their clinical data in an EHR and their administrative data (including payment information and data that would qualify as "health care operations") in their practice management (PM) system. Satisfying an accounting of disclosures for TPO requests in most practices is not a simple keystroke. As discussed more fully below, MGMA members have made it clear that completing these types of reports requires a substantial amount of manual collection from multiple data sources.

MGMA has conducted two surveys on the issue of accounting of disclosures, one in 2010 in response to the earlier OCR RFI on accounting of disclosures and a second in January 2019 in response to the current OCR RFI. When physician practice leaders were asked in 2010 how many requests of PHI disclosures they had received in the previous 12 months, it was clear that very few patients have made a request for an accounting of disclosures from their physician practice. As indicated in Table 1, almost 70 percent of respondents indicated that they had never had a request with an additional 22 percent reporting 1 to 10 requests from patients for an accounting of disclosures in the previous 12 months.

Table 1

2010 Question	Approximately how many requests for PHI disclosure accounting reports has your practice received from patients in the past 12 months?
Zero	69.1%
1 to 10	22%
11 to 50	2.9%
51-100	.6%
101-500	.9%
501 or more	0%
Do not know	4.6%

When we reprised this question nine years later, the results were very similar. As indicated in Table 2, almost 68 percent stated that their organization had received no requests for an accounting of disclosures with a further 17.8 percent indicating between 1 and 10 requests from patients in the past year. A further 4.4 percent responded that they had received 11 to 50 requests in the past year. A very small percentage (2.8 percent) indicated that they had received more than 50 requests in the preceding 12 months.

Table 2

2019 Question	Approximately how many of your patients have requested an accounting of PHI disclosures report in the past year?
Zero	67.9%
1 to 10	17.8%
11 to 50	4.4%
51 to 100	.3%
101 to 500	.9%
More than 500	1.6%
Unsure	7%

Timing of accounting of disclosures

OCR Questions

- *How much time do covered entities take to respond to an individual's request for an accounting of disclosures?*
- *How many worker-hours are needed to produce the accounting?*
- *What is the average number of days between receipt of a request and providing the accounting to the requesting individual?*
- *How would these estimated time periods change, if at all, if covered entities were to provide a full accounting of disclosures for TPO purposes? What is the basis for these revised estimates?*

MGMA Response

We have not surveyed members regarding the exact amount of time it takes to currently complete an individual's request for an accounting of disclosures, but anecdotally we have heard that the process is extremely onerous. Should the accounting of disclosures be expanded to include TPO, the effort to produce a report would increase exponentially. Most likely practices would be required to hire additional staff whose sole task would be to compile these reports. Further, in cases where a patient may have been seen multiple times over the required reporting period at a larger practice (utilizing perhaps numerous services and locations), the document given to the patient could literally be hundreds of pages in length and virtually indecipherable for the patient.

OCR Question

- *If your covered entity does capture and maintain information about TPO accounting, even though it is not currently required by the Privacy Rule, what is the average number of TPO disclosures made by the entity for a given individual in a calendar year? How many such disclosures are made from EHRs?*

MGMA Response

As we outline in Tables 1 and 2, the number of patient requests for an accounting of disclosures is extremely small. Our statistics include those requests made by the patient for an accounting of disclosures that would include TPO. The vast majority of these requests would be made to practices that have implemented an EHR.

OCR Questions

- *Should the Department require covered entities to account for their business associates' disclosures for TPO, or should a covered entity be allowed to refer an individual to its business associate(s) to obtain this information?*

- *What benefits and burdens would covered entities and individuals experience under either of these options?*

MGMA Response

It would be a significant burden should OCR decide to require practices to account for their business associates' disclosures for TPO. Smaller practices have multiple business associates and larger organizations may have dozens of business associates. Tracking TPO disclosures for each one of these business associates would be overwhelming for a practice and would serious disruption practice operations. Patients should be directed by the practice to the business associate to obtain this type of information.

OCR Questions

- *Is the system able to distinguish between "uses" and "disclosures" as those terms are defined under the Privacy Rule at 45 CFR 160.103? (Note that the term "disclosure" includes, but is not limited to, the sharing of information between a hospital and physicians who may have staff privileges but who are not members of its workforce).*
- *If the existing system only records access to information without identifying whether such access represents a use or disclosure, what information is recorded about each instance of access? How long is such information retained? What would be the burden for covered entities to retain the information for three years? Once collected, what additional costs or other resources would be required to maintain the data for each subsequent year? At what point would retention of the information be excessively burdensome? OCR requests specific examples and cost estimates, where available.*
- *If the system is able to distinguish between uses and disclosures of information, what details regarding each disclosure are automatically collected by the system (i.e., collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the disclosure or accessing the information?*
- *If the system is able to distinguish between uses and disclosures of information, what data elements are automatically collected by the system for uses (i.e., collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the use?*
- *If the system is able to distinguish between uses and disclosures of information, does it record a description of disclosures in a standardized manner (for example, does the system offer or require a user to select from a limited list of types of disclosures)? If yes, is the feature being utilized? What are the benefits and drawbacks?*
- *To what extent do covered entities maintain a single, centralized EHR system versus a decentralized system (e.g., different departments maintain different EHR systems, and an accounting of disclosures for TPO would need to be tracked for each system)? To what extent are covered entities that currently use decentralized systems planning to migrate to centralized systems or vice versa? How is the industry mix of centralized and decentralized systems likely to change over the next five or ten years?*
- *Do existing EHR systems automatically generate an accounting of disclosures under the current Privacy Rule (i.e., does the system account for disclosures other than to carry out TPO)? If so, what would be the additional burden to also account for disclosures to carry out TPO? If not, to what extent do covered entities use a separate system or module to generate an accounting of disclosures, and does the system interface with the EHR system? OCR requests cost estimates, where available.*

MGMA Response

MGMA asserts that this onerous new requirement on physician practices will be extremely difficult

to achieve without an enormous outlay of human and financial resources. These resources would be better utilized by physician practices to provide direct patient care. This mandate would run counter to the nation's efforts to improve patient care and reduce waste and inefficiency through administrative simplification and adoption of EHRs.

As shown in Table 3, just 22.1 percent of 2019 respondents reported that their EHR is currently able to generate an accounting of disclosure report that does not include disclosures made for TPO. 43.5 percent indicated that their current EHR cannot generate this type of report.

Table 3

2019 Question	Is your EHR currently able to generate an accounting of disclosure report that does not include disclosures made for treatment, payment, and healthcare operations?
Yes	22.1%
No	43.5%
We do not have an EHR	8.8%
Unsure	25.6%

MGMA research from 2010, outlined below in Table 4, indicated that just 17.7 percent of respondents had EHRs capable of distinguishing between "use" and "disclosure." If you exclude respondents who were not aware of their EHRs functionality on uses and disclosures, a significant majority of respondents reported their EHR did not have the capability to make this distinction. This suggests that EHR software will need to undergo a costly modification, staff will need to be trained, and manual processes instituted for many practices. It is typically only the most sophisticated of EHRs that can readily distinguish between "uses" and "disclosures" of PHI. Smaller physician practices are generally less likely to have the software that would permit this type of distinction. As a consequence, these organizations would be forced to resort to a time-consuming and burdensome manual process.

Table 4

2010 Question	Is your EHR able to distinguish between "uses" and "disclosures" of PHI?
Yes	17.7%
No	41.4%
Do not know	40.9%

Another important consideration is the "payment" aspect of a potential expansion of the accounting of disclosures requirement. PM software does not capture the type of data required to be included in the proposed access report and it is highly unlikely that this type of software could ever be retrofitted to perform this task. Further, PM software is not currently certified through any government accreditation program and vendors are not covered entities under HIPAA and thus could not be mandated to produce this functionality.

Physician practices submit claims to health plans as a courtesy for their patients, and thus should not be saddled with unnecessary mandates such as a requirement to account for these disclosures. The unintended consequence of such a requirement could be that physician practices cease offering this convenient benefit for their patients, leading to an increased number of patients asked to pay in full at the time of treatment and responsible to obtain their own

reimbursement from the health plan.

We assert that there could also be an unintended consequence of requiring practices to track and disclose information relating to the claim payment cycle. The number of staff assigned to revenue cycle activities is often at least double that of clinical staff in a practice, which also means there are numerous individuals required to access a single patient's PHI for administrative purposes in a practice. The additional workload necessary to track every single PHI disclosure made in support of the revenue cycle process would be simply overwhelming for these organizations.

Similarly, conducting operations such as quality assessment and improvement activities, outcomes evaluation, development of clinical guidelines, case management and care coordination, and the contacting of health care providers and patients with information about treatment alternatives should not be subject to onerous reporting requirements.

OCR Question

If an EHR is not currently able to account for disclosures of an EHR to carry out TPO, what would be the burden, in time and financial costs, for covered entities and/or their vendors to implement such a feature?

MGMA Response

Our research indicates that accounting for TPO disclosures will present a significant burden on physician practices. Should these organizations be required to include to whom a disclosure was made (i.e., recipient) and the reason or purpose for the disclosure, it would most likely require costly new software, additional staff, and force the practice to manually track much of this information.

While it is challenging for physician practices to create a report identifying all TPO disclosures, to produce that report going back three years into the patient's medical and financial records would be extremely onerous. The results from our 2010 survey suggest there would be serious burdens associated with an expansion of the accounting of disclosures policy. As Table 5 indicates, fully, 74 percent of respondents stated that providing an accounting report for three years of patient data would be "extremely burdensome" or "very burdensome." Conversely, only 6.2 percent stated that providing an accounting report for three years of patient data would be "not very burdensome" or "not at all burdensome."

Table 5

2010 Question	How burdensome (i.e., cost, staff training, computer upgrades) will it be for your practice to retain and make available to patients PHI disclosure accounting information for treatment, payment, and health care operations purposes for three years?
Extremely burdensome	51.1%
Very burdensome	22.9%
Somewhat burdensome	12.1%
Not very burdensome	5.8%
Not at all burdensome	0.4%
Do not know	7.6%

When respondents were asked in January 2019 (Table 6) how burdensome would it be for their practice to produce a PHI disclosure accounting report for TPO that includes to whom the disclosure was made (i.e., clinical staff, billing staff) and the reason for the disclosure, 83 percent indicated it would be very or extremely burdensome.

Table 6

2019 Question	How burdensome (i.e., staff training, computer upgrades, staff time required to produce the report) will it be for your practice to produce a PHI disclosure accounting report for treatment, payment, or healthcare operations that includes to whom the disclosure was made (i.e., clinical staff, billing staff) and the reason for the disclosure?
Extremely burdensome	60.8%
Very burdensome	22.2%
Somewhat burdensome	10.8%
Not very burdensome	2.9%
Not at all burdensome	1%
Unsure	2.5%

Statutorily required balancing test and the administrative burden on providers

Under the HIPAA Privacy Rule, each individual has the right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date of the individual's request. Prior to passage of HITECH, that right did not extend to several types of disclosures, including TPO disclosures. The primary reasons for excluding disclosures for TPO were that patients "understand that information about them will be used and disclosed in order to provide treatment or obtain payment;" such an accounting "could be extremely long and detailed… far too detailed to adequately inform the individual;" and would "place a tremendous burden on the covered entities." 64 Fed. Reg. 59,918, 59,985 (Nov. 3, 1999).

HITECH amended the accounting of disclosures requirement to include even disclosures for TPO. Under HITECH, if a covered entity, such as a physician practice, utilizes an EHR, the organization would be required to account for TPO disclosures. Upon receiving a request for such a disclosure, the physician practice will be required to provide individuals with an accounting of disclosures of PHI which occurred within the three years prior to the date of the request.

While HITECH requires the HHS Secretary to adopt regulations that take into consideration the individual's interest in knowing how PHI is used and disclosed, the legislation also directs the Secretary to determine the administrative burden to covered entities providing the accounting. HITECH states that "[s]uch regulations shall only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individual in learning the circumstances under which their protected health information is being disclosed *and takes into account the administrative burden of accounting for such disclosures (*emphasis added)." 42 U.S.C. § 17935(c)(2) [or Section 13405(c)(2)].

OCR Question

- *For covered entities already planning to adopt new EHRs, to what extent would a requirement to track TPO disclosures affect the cost of the new system?*

MGMA Response

It is important to note that producing a report listing TPO disclosures (who, when, and why) is not something even the most sophisticated EHR technology offers now. It would require a complete re-engineering of the software and it's highly likely that not all software vendors could or would offer this functionality. If the software vendor was to somehow create this capability, we anticipate the increased cost to practices would be so substantial as to act as a significant barrier to initial purchase or upgrade to a version with this functionality.

Accessing and reporting audit log data in practice systems is not currently a fully automated process, and, in many systems, cannot be easily done. Systems where electronic designated record sets are maintained may have very different capabilities, levels of data, technical platforms, and different ways of identifying patients, tracking and indexing audit data, and producing output. Aggregating access log data across multiple internal systems would be administratively and financially burdensome. These systems would require significant development and reconfiguration to enable the capability to efficiently produce and compile the necessary information to consolidate and generate access reports. We predict that a sizable percentage of software vendors, primarily the vendors serving smaller and rural practices, will either not have the capability to modify existing software to meet this requirement or will not be able to offer the modification at a price that is affordable to the practice.

OCR Questions

- *A covered entity's Notice of Privacy Practices must inform individuals of the right to obtain an accounting of disclosures. Is this notice sufficient to make patients aware of this right? If not, what actions by OCR could effectively raise awareness?*
- *Why do individuals make requests for an accounting of disclosures under the current rule?*
- *Why would individuals make requests for an accounting of TPO disclosures made through EHRs?*

MGMA Response

Due to the incredibly low volume of report requests, we believe that the current level of education regarding a patient's right to an accounting of disclosures contained in a practice's privacy notice is sufficient. Patients appear most concerned with cases where they do not want their medical record disclosed to a specific individual who is staff at a practice. This concern applies now and would apply even if the regulations were expanded to require the covered entity to provide the patient with all TPO disclosures. For example, a patient may know that a neighbor works at the facility they are visiting and may wish that this individual not have access to their medical record. Under current law, the patient is permitted to ask the practice not to disclose the record to this individual. Thus, the issue can be solved proactively, prior to the visit, as opposed to the patient requesting to see if the neighbor had accessed their medical record after the visit occurred.

We do not believe patients have any interest in receiving a lengthy (potentially hundreds of pages) report explaining which practice staff looked at their medical record for purposes of treating them, submitting their claim to insurance to limit their out of pocket expenses, or for performing healthcare operations such as quality measurement. We would encourage OCR to focus educational efforts aimed at patients and covered entities on the right of the patient to request that their medical record not be disclosed to a designated individual.

OCR Questions

- *What data elements should be provided in an accounting of TPO disclosures, and why?*
- *How important is it to individuals to know the specific purpose of a disclosure—i.e., would it be sufficient to describe the purpose generally (e.g., for "for treatment," "for payment,"*

or "for health care operations purposes"), or is more detail necessary for the accounting to be of value?

- *To what extent are individuals familiar with the range of activities that constitute "health care operations?" On what basis do commenters make this assessment?*

MGMA Response

As we state above, we do not believe there is a compelling need for patients to have a right to an accounting of disclosures report that includes TPO. When a patient comes to a physician practice with an issue or illness, it is with the expectation that practice staff will address their issue or treat their illness. If the patient does not wish practice staff to document the encounter or review their previous medical record, then they have the right to request this. However, the practice also has the right the refuse this request, as documentation is required for treatment, billing, liability, payment, and other purposes. Patients also have the right not to visit a specific care setting, if they have a specific privacy concern.

Similarly, as part of the typical revenue cycle process, practices will submit claims on behalf of the patient directly to the insurance carrier. This task is done as a courtesy to the patient and alleviates the burden on the patient of paying in full at the time of service and then submitting claims on their own to their insurance carrier after the encounter. As part of this process, practices use PHI to verify insurance eligibility, either manually (fax, phone), semi-manually (via insurance carrier web portal), or through an automated process (using the X12 270/271 electronic transactions). Again, practices perform this task as a courtesy to the patient as it can establish eligibility for a specific service or test and provides the patient with an estimation of their out-of-pocket expenses and furthering the administration's current aim of increasing transparency of healthcare costs. Other revenue cycle transactions also require practice staff to potentially access patient PHI, including prior authorization, claim status, acknowledgements, remittance advice, and claim payment.

In terms of healthcare operations, numerous practice staff are typically involved administrative, financial, legal, and quality improvement activities that are necessary for a practice to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, include:

- "Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity."

For physician practices, especially larger organizations, these tasks are handled by separate departments or individuals. Thus, the number of revenue cycle and healthcare operations staff who would access PHI for healthcare operations is significant. Tracking not only who has accessed this information and when but for what purpose would not only be extremely burdensome on practices but would yield next to nothing of value to the patient.

OCR Questions

- *How frequently do individuals who obtain an accounting of disclosures request additional information not currently required to be included in the accounting (e.g., information about internal uses or about disclosures for TPO)?*
- *What additional information do they request, and do covered entities provide the additional information? Why or why not?*

MGMA Response

As our 2019 survey results highlight, practices receive very few requests for an accounting of disclosures report. Even fewer patients request that the report include additional information that is not currently required in the accounting.

OCR Questions

- *If covered entities are unable to modify existing systems or processes to generate a full accounting of disclosures for TPO (e.g., because modification would be prohibitively costly), should OCR instead require covered entities to conduct and document a diligent investigation into disclosures of PHI upon receiving an individual's request for an accounting of disclosures for TPO?*
- *If not, are there certain circumstances or allegations that should trigger such an investigation and documentation by a covered entity?*
- *How much time should a covered entity be allowed to conduct and provide the results of such an investigation?*

MGMA Response

Should OCR require those practices who would be unable to modify their systems or processes to conduct and document a diligent investigation into disclosures of PHI upon receiving an individual's request for an accounting of disclosures for TPO, it would lead to significant burden.

To reiterate, the likely scenario that would trigger a request would be patient concern regarding an individual staff member having had access to their medical record. In these specific and rare instances, practices typically will work with the patient to identify and report any disclosure issues pursuant to the patient's concern. These are "ad hoc" investigations and should not be mandated through regulation. Practices, however, could be encouraged to provide this type of investigative process for those patients who request it.

OCR Questions

- *If OCR requires or permits covered entities to conduct an investigation into TPO disclosures in lieu of providing a standard accounting of such disclosures, what information should the entities be required to report to the individual about the findings of the investigation?*
- *For example, should OCR require covered entities to provide individuals with the names of persons who received TPO disclosures and the purpose of the disclosures?*

MGMA Response

We are concerned that a potential accounting of disclosures report to the patient could include specific names of individuals within the practice (or any other business associate or covered entity) and the action they took. Releasing this level of information raises important security concerns for those individuals who may become targets for discontented patients or family members. Healthcare providers and other covered entities must on occasion make decisions about treatment, authorizations, and other issues that patients may not understand without proper explanation from the practice t. This could lead to unwarranted threats, harassment or even potential physical harm to workforce members.

Being required to provide patients with specific names could also have the effect of discouraging legitimate access of medical records (for example, psychiatric notes) for fear of patient retaliation. There is also a concern that an accounting of disclosures report could include the time of the access. The original proposed rule also set out that the report could track access for the previous three years; we contend that the specific time of the access becomes unnecessary very soon after the access occurs. Thus, there is virtually no value in knowing that the access occurred at 3:15 p.m. on a date three years ago.

In responding to a patient's request for a report, it would be reasonable to provide the patient with the date of the creation of the patient's record in the EHR and an aggregate total count of actions taken on the patient's record, such as the number of EHR record creations, modifications, viewings, and printings within a specified period of time. In making any disclosures to patients, OCR should permit practices the latitude and discretion to limit the specificity of disclosures. This is particularly important in those cases where the disclosures are inadvertent (though innocuous and do not rise to the level requiring a breach of PHI notification).

There are no readily known parallel requirements to disclose the names of specific persons who access an individual's personal data in other industries that handle sensitive information. The financial industry, for example, does not provide this information—for the same security reasons we expressed earlier. An example of a related type of information disclosure would be the financial credit report provided to consumers upon their request. While these credit reports include the name of the entity accessing the individual's credit history, the report does not include the specific names of the employees at that entity that requested or accessed the financial information.

OCR Questions

- *The HITECH Act section 13405(c) only requires the accounting of disclosures for TPO to include disclosures through an EHR. In its rulemaking, should OCR likewise limit the right to obtain an accounting of disclosures for TPO to PHI maintained in, or disclosed through, an EHR? Why or why not?*
- *What are the benefits and drawbacks of including TPO disclosures made through paper records or made by some other means such as orally?*
- *Would differential treatment between PHI maintained in other media and PHI maintained electronically in EHRs (where only EHR related accounting of disclosures would be required) disincentivize the adoption of, or the conversion to, EHRs?*

MGMA Response

While an accounting of disclosures based on TPO parameters would be an incredible burden on its own, a requirement to include i TPO disclosures made through paper or oral discussion would be an overwhelmingly challenge and we urge these concepts be rejected.

Practice workflow includes minute by minute interactions between clinical and administrative staff. A single patient encounter would involve multiple "touch" points via the EHR, paper, and oral

communication. The delivery of patient care would literally grind to a halt if every staff interaction had to be recorded (who, when, and why) and maintained for years, just on the minute chance that a patient might request a report.

OCR Question

Please provide any other information that OCR should consider when developing a proposed rule on accounting of disclosures for TPO.

MGMA Response

MGMA concurs with the agency's contention that the 2011 proposed access report requirement would create undue burden for covered entities without providing meaningful information to individuals. Therefore, we strongly support OCR's intention in this RFI to withdraw the 2011 proposed rule. We oppose, however, any attempt to mirror the provisions of the 2011 proposed rule in future rulemaking.

Current law protects the patient

OCR should closely review how a combination of current and enhanced patient rights could achieve the goal of providing individuals with the ability to effectively control their health information, without imposing an undue burden on providers. Under the current HIPAA Privacy Rule, practices and other covered entities are required to monitor and audit access to PHI. In addition, should an improper use or disclosure of PHI be discovered, even if that disclosure was the result of internal misuse by a member of the practice staff, the practice has an obligation to report such misuses to the individuals whose PHI was involved.

HIPAA permits a patient to complain to a practice should the patient have a specific concern regarding how their PHI was handled. Should a patient have a concern about a particular staff member at a practice, the patient may request that the practice restrict that employee's access to the patient's PHI. Therefore, existing requirements already provide sufficient mechanisms for patients to learn of and manage accesses by practice staff members when there is actual misuse or a concern of misuse.

Enhancements to this current approach could include augmenting the ability of practices to investigate potential inappropriate disclosures, improved covered entity training, revised privacy notices, and patient education regarding their ability to request that the covered entity restrict access to their health information.

Section D: Notice of Privacy Practices

OCR Question

- *What is the burden, in economic terms, for covered health care providers that have a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's NPP? OCR requests estimates of labor hours and any other costs incurred, where available.*
- *For what percentage of individuals with whom a direct treatment provider has a relationship is such a covered health care provider unable to obtain an individual's written acknowledgment?*
- *What are the barriers to obtaining it?*
- *How often are NPPs bundled with other documents at patient "intake" and with how many other pages of documents?*

- *How often are NPPs printed with non-NPP materials, either on the same page, or as a continuation of one integrated document, or as being physically attached to other documents?*
- *What is the nature of these non-NPP materials?*
- *How often, if at all, are covered health care providers required to have the patient sign updated versions of these forms (e.g., annually, each visit, no subsequent updates required)?*
- *Are electronic signatures permitted for these forms? If so, does this make the process less burdensome?*
- *For what percentage of individuals with whom a direct treatment provider has a relationship is such a covered health care provider unable to obtain an individual's written acknowledgment?*
- *What are the barriers to obtaining it?*

MGMA Response

While we are not able to supply specific estimates of labor hours and other costs incurred, practices with a direct treatment relationship with an individual generally report that the process of obtaining and storing a written acknowledgment of receipt of the practice's NPP somewhat burdensome. Typically, new patients coming to a practice will be required to complete a number of forms prior to being seen by clinical staff. The written acknowledgement of receipt of the NPP is typically included in this set of intake forms. The number of forms a patient is required to review and sign at intake varies by medical specialty and organizational preference. The lengthiest form is most often the one that captures demographic information, current and past medical history, medications, and allergies, and family medical history. Additional intake materials might include the practice no-show policy, a Medicare Advanced Beneficiary Notice, an explanation of the practice's participation in an ACO or other payment model, medical records release, authorized representative, practice policy regarding telephone and email communications, and others.

Where the written acknowledgement of receipt of the practice's NPP becomes significantly more challenging is in cases where the patient is not physically seen at the location, for example, those with telehealth capabilities. Other challenges include confusion on the part of the patient regarding what the purpose of the written acknowledgement of receipt of the NPP. Some patients express concern that the form releases the practice of all obligations to protect the patient's PHI or permits the practice to disclose PHI indiscriminately. While these concerns may be misplaced they still do require practice staff to take time to explain the purpose of the acknowledgement and verbally explain the privacy rights of the patient and obligations of the practice.

The written acknowledgement of receipt of the NPP is typically a stand-alone document and not combined with other forms requiring a patient signature. Some practices are now offering the patient electronic versions of the intake forms, including the written acknowledgement of receipt of the NPP. In these cases, the patient will review the acknowledgement on a screen and electronically sign.

Practices vary with respect to how frequently they have patients sign a written acknowledgement of receipt of the NPP. Some have made the decision to update all forms at the beginning of each year, and have their patients sign a new acknowledgement every 12 months. Other practices rely on the original written acknowledgement of receipt of the NPP and only collect written acknowledgements from new patients.

There is also administrative burden associated with storing the completed acknowledgement form. It must be kept with the patient record and accessible upon request for production. Adding to burden is when the patient does not sign the form, and the practice has made a "good faith" effort to obtain the signature. There must be included in the patient's medical record a note explaining why the patient was unable or unwilling to sign the written acknowledgement of receipt

of the NPP, the efforts the practice went through to obtain it, the reason why it was not obtained, and the date.

Adding to the administrative burden associated with the acknowledgement of receipt, should the practice be required to make a "material change" to the contents of its NPP, the revised NPP would need to be provided again to patients and a new acknowledgement form obtained and stored.

One opportunity to reduce the burden associated with obtaining and maintaining the written acknowledgement of receipt of the practice's NPP would be to waive this requirement should the covered entity post the NPP in a prominent and public area of their facility and on their website. By requiring the NPP to be posted on the website, this waiver could then apply to those organizations offering services that would not require the patient to be physically present at the time of service.

OCR Question

If NPP training is part of your general annual training, how much of this training cost do you estimate your organization spends to train covered entity staff on their obligations to seek and maintain documents related to the NPP acknowledgment requirements?

MGMA Response

As required by law, practices regularly train clinical and administrative staff on the organization's HIPAA Privacy and Security policies and procedures. As part of that training, staff are typically educated regarding the requirement to obtain written acknowledgment of receipt of the NPP or documentation that a good faith effort was made to obtain the acknowledgment.

OCR Questions

- *What is the burden, in economic terms, for covered health care providers to maintain documentation of the acknowledgment or the good faith effort to obtain written acknowledgment and the reason why the acknowledgment was not obtained?*
- *What alternative methods might providers find useful to document that they provided the NPP?*
- *For example, to what extent would the use of a standard patient intake checklist reduce the burden?*

MGMA Response

Once they have obtained the written acknowledgement of receipt on paper, practices will typically store it in the patient record or scan the document into the PM or EHR. These tasks require time by administrative staff to complete. Some practices have moved to presenting these forms in an electronic format with electronic signature. This information is then captured in either the PM or EHR. More challenging is when the patient cannot or will not sign the acknowledgement of receipt. In these cases, practice staff would be required to make a good faith effort to obtain it. However, "good faith effort" is not explicitly defined so practices may allot significant time in an attempt to contact the patient and have them complete the form. Should the patient not sign the acknowledgement of receipt, staff must then fully document the efforts made to obtain the signature. These processes can be time consuming and distract from staff performing other more patient care-focused tasks.

While there have been industry efforts at standardizing the patient intake form, most notably by the Workgroup for Electronic Data Interchange (WEDI) with its "Virtual Clipboard" initiative, none have received widespread vendor and health plan acceptance or support from the federal government. Standardizing these types of forms and potentially providing a platform where

patients could capture and transmit demographic, insurance-related, and clinical data electronically would improve health outcomes while reducing cost and burden. We would encourage OCR to work with WEDI and others in the industry to advance the issue of standardized patient intake forms.

OCR Question

- *What use, if any, do covered health care providers make of the signed NPP forms, or documentation of good faith efforts at securing written acknowledgments, that the Privacy Rule requires providers to maintain?*

MGMA Response

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.

OCR Question

- *What benefits or adverse consequences may result if OCR removes the requirement for a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgment of the receipt of the provider's NPP? Please specify whether identified benefits or adverse consequences would accrue to individuals or covered providers.*

MGMA Response

In terms of covered healthcare providers and their use of the documentation, we believe there would be no adverse consequences if OCR removes this requirement, as patients rarely, if ever, review or modify their acknowledgement..

As a reminder, providers are currently required to make available to all their new patients a copy of the NPP and post the NPP in a public area of their facility and on the practice website, which provides sufficient notice to patients.

OCR Question

- *Are there modifications to the content and provision of NPP requirements that would lessen the burden of compliance for covered entities while preserving transparency about covered entities' privacy practices and individuals' awareness of privacy rights? Please identify specific benefits and burdens to the covered entity and individual, and offer suggested modifications.*

MGMA Response

It is common for practices to engage with their legal team in development of their NPP. Although the Privacy final rule outlined what contents are minimally required, each NPP must be tailored to meet the specific needs of an organization. As a result, many NPPs are fully "compliant" yet not easily read or understood by the patient. Modifying the requirements of the NPP would necessitate practices re-engaging with their legal teams to revise current NPPs and go through the process of distributing the revised NPP to all patients. This would needless create significant additional burden for practices.

An alternative approach would be outreach-focused. The model NPP produced by OCR is extremely well-constructed and very patient-focused. Rather than modify the required contents of

the NPP, we would recommend OCR engage with consumer and physician practice organizations to promote use of the OCR model NPP.

NPP models

OCR Questions

- *While covered entities are required to provide individuals an NPP, use of OCR's model NPPs is optional. Do covered entities use these model NPPs? Why or why not?*
- *OCR has received anecdotal evidence that individuals are not fully aware of their HIPAA rights. What are some ways that individuals can be better informed about their HIPAA rights and how to exercise those rights? For instance, should OCR create a safe harbor for covered entities that use the model NPPs by deeming entities that use model NPPs compliant with the NPP content requirements? Would a safe harbor create any unintended adverse consequences?*
- *Should more specific information be required to be included in NPPs than what is already required? If so, what specific information? For example, would a requirement of more detailed information on the right of patients to access their medical records (and related limitations of what can be charged for copies) be useful?*
- *Please identify other specific recommendations for improving the NPP text or dissemination requirements to ensure individuals are informed of their HIPAA rights.*

MGMA Response

MGMA again lauds OCR for its development of model NPPs. These are colorful, easy-to-read documents that convey the necessary information to patients. We also appreciate the fact that the model NPPs can be customized to meet the specific needs of individual practices. From our website (www.mgma.org/hipaa) we provide links to these model forms and as well as provide an additional sample NPP developed by MGMA. We have heard that the OCR model NPP has been well-received by physician practices.

Education is critical if patients are to be made aware of their rights under HIPAA. In many cases, patients often rely on their practice to provide this education. Some opportunities for OCR to assist in this education include:

- OCR could develop educational posters and post these on its website. These could mirror what CMS has produced to have practices post in their waiting rooms to educate patients regarding the new Medicare card initiative. Here is the CMS poster as a reference.

- Partner with provider organizations and patient advocacy groups on Webinars/educational sessions.

- Conduct "open door" type calls for provider organizations and include a Q/A component.

Section E: Additional Ways To Remove Regulatory Obstacles and Reduce Regulatory Burdens To Facilitate Care Coordination and Promote Value-Base Health Care Transformation

OCR Questions

In addition to the specific topics identified above, OCR welcomes additional recommendations for how the Department could amend the HIPAA Rules to further reduce burden and promote coordinated care.

- *What provisions of the HIPAA Rules may present obstacles to, or place unnecessary burdens on, the ability of covered entities and/business associates to conduct care coordination and/or case management? What provisions of the HIPAA Rules may inhibit the transformation of the health care system to a value-based health care system?*
- *What modifications to the HIPAA Rules would facilitate efficient care coordination and/or case management, and/or promote the transformation to value-based health care?*
- *OCR also broadly requests information and perspectives from regulated entities and the public about covered entities' and business associates' technical capabilities, individuals' interests, and ways to achieve these goals.*

MGMA Response

It is critical that OCR balance the need for patient information to move efficiently between care setting in support of care coordination and care transitions with the need that the data in transit be secure.

OCR Question

- *Additional Ways to Remove Regulatory Obstacles and Reduce Regulatory Burdens to Facilitate Care Coordination and Promote Value-Based Health Care Transformation*

MGMA Response

In addition to modifying appropriate provisions of the current Privacy Rule, MGMA encourages the agency to review the potential of decreasing regulatory burdens associated with the Security Rule that may be impeding the exchange of PHI for care coordination, case management, and value-based payment programs.

There persists significant confusion regarding the conducting of a security risk analysis and mitigating any identified risks. Ensuring flexibility in complying with the Security Rule is critical as there is a vast difference in technical and financial capabilities between smaller and larger physician practices. At the same time, there continues to significant confusion regarding what constitutes a "compliant" security solution.

ONC is actively engaged in the development of a nationwide health information exchange environment. Moving clinical data through these exchanges to support case management and care coordination is a centerpiece of ONC's interoperability efforts. Due to the heightened concern regarding the potential of unauthorized disclosures, practices, other covered entities and business associates are increasingly reluctant to disclose PHI to entities that are either not subject to the HIPAA Security Rule requirements, or do not appear to be sufficiently aware of them. We urge OCR to issue additional guidance and develop safe harbors for compliance with the HIPAA Security Rule so that covered entities and their business associates can have increased assurance that they (and their recipients) are meeting OCR's expectations from a security perspective.

<u>Modifying the OCR ransomware policy</u>
Ransomware presents a danger to physician practices and the patients they serve and we urge OCR to modify the current HIPAA Privacy and Security enforcement approach. We recommend moving away from a culture of "blaming the victim" to one focused on transparency and action. This revised approach will lead to improved cyber hygiene in the healthcare environment and a reduced threat to patient records and patient safety. When a practice is cyberattacked, care coordination and data sharing in support of patient care cannot occur.

Understanding how treacherous the current cyber environment is, OCR must have access to accurate information regarding the scope and nature of these attacks if the industry is to have any reasonable chance of effectively combating cyberterrorism. Real-time reports from physician

practices experiencing a cyberattack, understanding exactly what tactics these criminals are using and what software they are deploying, providing actionable information to affected organizations on how to combat the attack, and amassing the intelligence necessary to prevent future cyberattacks is extremely vital. Without access to these data, developing and implementing a strategy to counter these criminal acts becomes impossible. Unfortunately, due to current policy, there is reason to believe HHS may not have a comprehensive picture of the scope of cyberattacks in healthcare due to its punitive and disciplinary approach to ransomware attacks.

OCR currently considers a ransomware attack a data breach, and thus medical practices attacked by ransomware are subject to the same process for both notification and enforcement as laid out in the Breach Notification Rules contained in the 2013 HIPAA Omnibus regulation. We assert, however, that this equating of ransomware with a traditional breach of PHI is inappropriate and should be changed. Although the broad definition of a breach as an "impermissible use or disclosure of protected health information" may apply to certain ransomware attacks, we believe there are inherent differences between the two threats to PHI.

A type of malicious software (malware), ransomware is unique from other forms of cyberattack, with a specific goal of denying the victim access to their own data, as opposed to removing or copying data such as a medical record. Typically, a ransomware attack will encrypt a practice's data with a key known only to the hacker who inserted the malware. The hacker then demands a ransom be paid to release the data through use of a decryption key. In many cases, the perpetrator will instruct the victim to pay a ransom via an untraceable cryptocurrency, such as Bitcoin. In some cases, the healthcare sector has seen these criminals deploy ransomware with the ultimate goal of damaging or destroying patient data. Ransomware is therefore distinct from other breach-type events where PHI has been improperly disclosed to unauthorized individuals.

Physician practices, especially smaller organizations and those located in rural areas of the country, simply are not equipped to ward off sophisticated cyberattacks and typically do not have sufficient internal technical expertise or necessary budgets to effectively meet these new cybersecurity challenges, despite being committed to securing their data. While reporting data breaches is required under the 2011 Omnibus regulation, the advent of more sophisticated cyberattacks in more recent times demand a revised approach to reporting, transparency, and enforcement.

It is unreasonable and counter-productive for practices to be penalized by the federal government for a ransomware attack that is beyond their control. We are concerned that the threat of punitive measures being imposed by the federal government following a ransomware attack could act as a deterrent against reporting the event. It is also important to note that organizations experiencing a ransomware attack incur significant harm from the attack itself. The inability to access important data that a practice maintains can be catastrophic in terms of the lock out of sensitive patient information, disruption to regular operations (including the ability to treat patients), financial losses related to lost claims data, the expense incurred to restore systems and files, and the potential long-term harm to the reputation of the organization.

Ransomware is not typically a use or disclosure of PHI but rather extortion to unlock or regain access to data critical to the business. This new, insidious form of attack on our nation's care delivery settings demands a new approach to information gathering and enforcement action. Therefore, we urge OCR to adopt a ransomware policy that encourages medical practices to report cyberattacks and collaborate with the federal government in an investigation to mitigate the damage and ensure the safety of its patients. We recommend the following steps be taken to better address the ransomware threat to physician practices.

- Establish a new ransomware transparency and enforcement policy. Any physician practice, other HIPAA covered entity, or HIPAA business associate that voluntarily reports a ransomware attack should not be subject to OCR enforcement action related to that ransomware attack, nor should the impacted organization be required to be listed on the HHS Breach Portal regarding the specific ransomware attack reported.

- Create a process of voluntary real-time ransomware reporting. HHS should work with the appropriate executive agencies, such as the U.S. Department of Justice, to provide a platform where physician practices can voluntarily report a ransomware cyberattack as it is occurring or if it is suspected. This disclosure should not prompt disciplinary action under HIPAA unless there is evidence of recklessness on the part of the medical practice. Rather, this action should begin an urgent, cooperative investigation to preserve the integrity of the extorted data and study the attack to prevent further damage related to the malware.

- Develop an HHS website focused solely on cybersecurity for healthcare providers. This website should:

    - **Present the latest information on cybersecurity focused on the healthcare sector**. Recently, HHS developed the Healthcare Cybersecurity Communications Integration Center (HCCIC), which could act as a template for a provider-centric website. A number of high-level goals for the HCCIC were identified, including "Enhance(d) public-private partnerships through regular engagement and outreach." HHS also acknowledged that the HCCIC was an integral part of the Department's coordinated response to the 2017 WannaCry and Petya incidents, providing analysis on these threats and their impact on healthcare.

    - **Promote practical, easy-to-comprehend guidelines and best practices** to assist providers in understanding and preparing to meet cyber challenges. Provide cases studies of organizations impacted by cyberattacks including the type of attack, steps the organization took to detect the attack, measures taken to mitigate the impact of the attack on clinical and administrative operations, and contingency plans deployed to ensure minimal impact on patient care.

    - **Compile cybersecurity educational resources from federal agencies** such as OCR, the National Institute of Standards and Technology, the Centers for Medicare & Medicaid Services, the Office of the National Coordinator for Health Information Technology, the Federal Bureau of Investigation, and other applicable agencies. Making these resources available in a single location will greatly facilitate effective and efficient communication to provider audiences and greatly expand their dissemination.

- Expand educational outreach to providers. In recognition that cyberattacks represent a clear threat to the nation's healthcare delivery system, HHS should fully fund a cybersecurity educational outreach program aimed at providers, with specific emphasis on small and rural physician practices. Communication vehicles could include "open-door" telephone forums, newsletters and bulletins, interactive webinars featuring cybersecurity experts, and face-to-face presentations at provider meetings. We encourage HHS to engage directly with MGMA and other appropriate provider organizations to solicit feedback regarding educational content and outreach strategies.

Conclusion

Creating additional caveats restricting physician's abilities to disclose and receive PHI for, treatment, payment, or healthcare operations unnecessarily complicates HIPAA regulatory compliance, frustrates care coordination, and increases burden on practices. As our healthcare system evolves toward value-based care, care coordination among providers is paramount. To best position practices for success, clinicians within a value-based network require timely access to a patient's entire medical record to provide safe and high-quality treatment. Compliance with multiple restrictions on patient PHI sharing is unnecessary and impedes this flow of information.

We are hopeful that, if implemented appropriately, modifications to the current HIPAA Privacy and Security Rules could enhance the ability of physician practices to engage in care management and care coordination activities, both integral to a successful value-based approach. OCR has outlined a broad set of potential issues for regulatory actions. We encourage the agency to pinpoint those aspects of the current law that negatively impact the appropriate sharing of clinical data in support of patient care and those issues that add unnecessary administrative burden on physician practices. We strongly caution OCR against reducing the time permitted for practices to provide the patient their designated record set, support the rescinding of the 2011 Notice of Proposed Rulemaking on expanding the accounting of disclosures report requirement, and oppose expansion of the current accounting report requirement as this would impose a significant new burden on practices with no discernable benefit to the patient.

We appreciate the opportunity to share our perspective regarding OCR's review of the current HIPAA Rules and offer recommendations to help shape the direction of potential new policy. Should you have any questions, please contact Robert Tennant at rtennant@mgma.org or 202-293-3450.

Sincerely,

/s/

Anders Gilberg, MGA
Senior Vice President, Government Affairs