May 30, 2019

Donald Rucker, MD
National Coordinator
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

RE: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Dear National Coordinator Rucker:

The Medical Group Management Association (MGMA) is pleased to submit the following responses to the Office of the National Coordinator for Health Information Technology (ONC) Proposed Rule, *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program.* This regulation seeks to move the health care ecosystem in the direction of interoperability and to meet the vision outlined in the bipartisan 21st Century Cures Act (Cures Act) to improve access to, and quality of, information that physician practices and others require in order to make informed healthcare decisions. We commend ONC for recognizing the need to improve interoperability to increase access to healthcare information and for seeking stakeholder feedback on how this best can be accomplished.

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 40,000 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.

ONC has proposed an extremely ambitious set of requirements for physician practices and health IT developers. We support many of the Administration's health IT goals, particularly putting patients at the center of the care delivery process by arming them with the health information they need. Our hope is that interoperability, if appropriately implemented, will permit physician practices and other care providers to gain quicker access to more accurate and pertinent patient information. This transformation could lead directly to enhanced efficiency and improved clinical performance.

MGMA appreciates the intent of the ONC Proposed Rule and the promise that health IT offers physician practices. However, as Senate Health, Education, Labor and Pensions Committee Chairman Lamar Alexander reminded the Administration at the May 7 hearing *Implementation of the 21st Century Cures Act: Making Electronic Health Information Available to Patients and Providers, Part II*, "…if you play it a little slower, you're less likely to make a mistake." We urge ONC to avoid pushing physician practices too far, too fast. The risks of moving too quickly include additional administrative and financial burdens on practices, weaker privacy and security protections for sensitive health information, an increased level of physician burnout, and the potential of compromised patient care.

To ensure ONC's regulations better fulfill the interoperability intent included in the Cures Act, ONC should consider staging the final requirements in such a way that: (i) practices and their vendor partners have sufficient time to develop and implement software solutions; (ii) compliance with the requirements do not result in undue administrative burden on practices, as stipulated in the Cures Act; (iii) data quality is promoted above data quantity; and (iv) appropriate privacy and security provisions are paramount in the deployment of Application Programming Interfaces (APIs) and other interoperability provisions.

We submit the following recommendations to assist in facilitating safe, effective, secure, and interoperable health IT.

SUMMARY OF RECOMMENDATIONS

- **Avoid overly aggressive mandates.** Imposing stringent new mandates with an overly aggressive implementation timeframe could be counterproductive by increasing administrative and financial burdens on physician practices, threatening the security of health information, and potentially compromising patient safety.

- **Release interim final rule and extend implementation timeline.** Due to the significance and breadth of this rule, the next round of regulations should be released as an interim final rule. We also recommend ONC provide additional time for physician practices and other impacted entities to come into compliance with the regulatory provisions.

- **Consider the unintended impact on the QPP.** The CMS Quality Payment Program (QPP) and, in particular, the Merit-based Incentive Payment System (MIPS), are the primary vehicles driving practices to implement modified 2015 Edition Certified EHR Technology (2015 CEHRT). Should ONC finalize overly stringent requirements with administrative burdens and costs, clinicians may be unable to participate in the Promoting Interoperability component of MIPS, resulting in lower QPP scores or penalties.

- **Create a new CEHRT edition.** The proposed EHR certification requirements are robust enough to warrant a new edition. Rather than continue calling it the 2015 Edition, we recommend it be renamed the 2020 Edition. This step would aid practices during the vendor contracting process and avoid situations where practices were sold 2015 Edition CEHRT that did not meet the modified requirements set forth in this rule..

- **Develop a tiered approach to data release.** We recommend ONC develop a 5-tier approach to the release of patient information. Our approach seeks to more effectively identify exactly what information the patient is requesting and reduce the administrative burden on the practice required to produce it.

- **Require third-party app developers sign BAAs.** To better ensure that appropriate security measures are in place, MGMA recommends ONC require app development companies to obtain a business associate agreement (BAA) with practices. A BAA would create a safe harbor from liability for practices if health information is disclosed by a third-party and unauthorized by the patient.

- **Exclude those not participating in the QPP.** ONC should not to require clinicians who are not eligible for participation in the QPP Program to be subject to these requirements as they are likely not to have implemented 2015 CEHRT. At a minimum, these clinicians should be given at least 24 additional months to comply.

- **Narrow the definition of EHI, particularly excluding payment.** The definition of electronic health information (EHI) is simply too broad and will lead to increased administrative burden and industry misunderstanding regarding what health data must be disclosed. The definition of EHI should closely mirror the existing definition of "designated record set" and not include payment.

- **Avoid complex information blocking requirements.** MGMA recognizes the importance of limiting information blocking, but the approach proposed by ONC is far too complex. It would significantly increase administrative burden for physician practices, cause industry confusion regarding what data can be disclosed and when, and increase the risk for sensitive health information to be shared inappropriately or not shared when needed. Rather than subject providers to information blocking penalties, we recommend ONC engage in an educational campaign to better inform clinicians and their patients regarding their rights and responsibilities vis-à-vis information exchange. The final regulation should be reasonable, actionable, and not add needless administrative burden.

- **Support for the USCDI.** MGMA agrees with ONC's proposal to require all certified EHRs to support the U.S. Core Data for Interoperability version 1 (USCDI v1). ONC should establish a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on any proposed expansion of the USCDI.

- **Adopt API standards.** MGMA generally agrees with ONC's proposal that certified EHRs must support new requirements around API design, function, and use to improve interoperability. We concur with the agency's proposal to adopt Fast Healthcare Interoperable Resources (FHIR) Release 4 and compliance with Health Level 7 U.S. Core FHIR Implementation Guides.

- **Secure patient data transmitted via APIs.** While MGMA supports the use of APIs to enhance interoperability and give patients access to their health information, we are concerned about the security implications with the deployment of APIs. Absent appropriate privacy protections, we believe patient information is at risk of being sold, used for vendor marketing, and shared without permission with third parties.

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

- **Implement a reasonable vendor fee structure and process.** ONC must address the potential of excessive fees that practices will be charged by EHR vendors to connect their products with other health IT systems, health information exchanges, and third-party applications. While we appreciate the agency's attempt to limit permissible fees, we urge the adoption of a tiered fee structure for APIs. We also recommend oversight of the vendor sector and the creation of toll-free numbers, email addresses, and a website where practices can lodge fee-based complaints directly to ONC.

- **Permit clinician use of professional judgement.** ONC should allow clinicians to use their professional judgement to protect their patients' privacy rights, including the designation for what constitutes "minimum necessary."

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

- **Increase EHR oversight.** We oppose any plan to reduce oversight of EHR software or real-world testing. Physician practices need assurance that the software they purchase meets the requirements set out in the ONC certification. We urge ONC to ramp up its surveillance of health IT vendors for compliance with ONC certification requirements, security protocols, and appropriate fee charges.

- **Standardize patient demographic data.** Regarding the patient matching request for information, accurate patient matching is critical if physician practices are to rely on the transmitted data. To improve patient matching, we recommend ONC support the standardization of demographic data, including applying the U.S. Postal Service Standard to the address field. We also encourage exploring the use of email address as an additional patient matching element.

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

COMMENTS ON SPECIFIC PROVISIONS OF THE PROPOSED RULE

Implementation Timing

ONC Proposal (Page 7429)

Going forward, health IT developers would be required to amend their contracts/agreements to remove or make void the provisions that contravene this Condition of Certification within a reasonable period of time, but not later than two years from the effective date of a subsequent final rule for this Proposed Rule.

MGMA Response

The proposal that ONC has laid is extremely ambitious and will significantly impact physician practices and their vendor partners. Fully implementing the requirement in this regulation will force practices to invest considerable resources in technology upgrades and retooling workflows. The incentive dollars associated with the QPP that intended to defray the cost of technology upgrades has largely evaporated.

In order to meet regulatory requirements, practices must rely heavily on their EHR vendors to meet the regulatory requirements. Practices using EHR products with a smaller market footprint are particularly vulnerable should their vendor not upgrade their software to support the new

certification criteria. The final timeline the agency develops should reflect the reality of today's practice environment.

We recommend the following implementation approach when moving forward with final requirements:

- Permit additional opportunity for the industry to provide input by issuing the next stage of the rulemaking process as an interim final rule.

- Survey the EHR vendor community to accurately determine what products will be upgraded, which will not, and expected timing for re-certifications.

- Allow for a minimum of a 36-month implementation period following publication of a final rule.

ONC Proposal (Page 7513)

Electronic Health Information (EHI) means— (1) Electronic protected health information; and (2) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual…To be clear, this definition provides for an expansive set of EHI, which could include information on an individual's health insurance eligibility and benefits, billing for health care services, and payment information for services to be provided or already provided, which may include price information.

MGMA Response

ONC proposes to define the term EHI to include electronic protected health information (as defined by HIPAA) and any other electronic information that identifies an individual and relates to the past, present or future health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. We believe that the proposed definition of EHI is too broad and, coupled with the information blocking component of the Proposed Rule, will complicate and obscure the intent of the law, which was to give patients and providers actionable information to assist in the care delivery process.

ONC should narrow the definition of EHI in the final rule as this definition will be critical for practices navigating information blocking restrictions or conditions of certification requirements. The EHI definition as proposed could result in the following unintended consequences:

- If a developer of certified health IT elects to develop and offer a registry of health information for research or quality assurance *separate* from its certified health IT, the developer would be subject to the information blocking restrictions with respect to both its electronic health record *and* the research/QA registry. Meanwhile, an entity that does not have a certified health IT product may create a registry of health information for research or quality assurance and would not be subject to the information blocking restrictions. There is no public benefit to treating two otherwise similar registries differently.

- If a developer of certified health IT "produces and electronically manages" EHI, the developer may be required under the Proposed Rule to develop and obtain certification for an "EHI Export" mechanism, even if the EHI is "produced or electronically managed" in a separate registry or database from the developer's certified health IT. This means, for

example, that if the developer wanted to develop a health IT solution separate and apart from its certified health IT to permit a patient safety organization to collect and track case reports, the developer would potentially need to obtain certification from an ONC-approved certification body to ensure the product contained certified EHI export functionality.

To avoid these and other unintended consequences of such a broad definition for EHI, we recommend that ONC limit the definition to identifiable information maintained electronically in a designated record set to better capture the universe of information that Congress sought to protect in the Cures Act.

Inclusion of "Payment" in the EHI Definition

We are very concerned with including in the definition of EHI "the past, present or future payment for the provision of health care to an individual." The definition uses the term "payment" but does not fully define that term. Would this definition include, for example, each of the transactions conducted by the practice in the revenue cycle that generates the payment? If this is the case, a practice would be responsible for collecting, maintaining, and producing each of the transactions (both manual and automated) that culminated in the "payment." These would include, insurance eligibility verifications, prior authorizations, claim status inquiries, acknowledgement transactions, claims, remittance advice, and payment.

Requiring the transmitting of "payment" data would impose an almost untenable administrative burden on practices and offer little value to the patient. The transaction information conveyed by the practice, with its ASC X12 terminology, CPT and ICD codes, would be indecipherable to most patients. Further, claim information by design precisely mirrors the information included in, and thus duplicative of, the medical record. Finally, most practices, particularly smaller organizations, leverage billing services and/or clearinghouses for revenue cycle transactions, receipt of paper or electronic remittance advice, and even the health plan payment itself. The administrative burden and cost manually tracking transactions from these third parties would be significant and the retrieval process itself would be extremely lengthy.

Patient Access to EHI

In the Proposed Rule, ONC outlines the type of EHI that a practice would be required to produce for a patient or other authorization entity, but the rule does not stipulate how quickly the information must be provided. The perception that a practice can simply press a button and immediately download all EHI is inaccurate. Practices typically store information in multiple locations and in multiple formats. Larger practices can have patient-identifiable data in literally hundreds of locations and formats. Producing a record to fulfill a patient request can be an onerous and time-consuming task.

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 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:

- Protected Health Information (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 and the practice must agree if it is reasonable. 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 could 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.

While some individual access requests should be relatively easy to fulfill, the HIPAA Privacy Rule recognizes that there may be other circumstances where additional time and effort is necessary to locate and format the requested PHI.

The Privacy Rule is intended to set the outer time limit for providing access, not indicate the desired or best result. 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, if that is feasible). However, in the majority of instances, 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.

MGMA recommends 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 their rights under HIPAA to access their medical record (or a specific component of the record).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 Medicaid 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 practices with patient portals but without 2015 Edition CEHRT.

Scope of EHI to be Provided to the Individual

ONC Proposal (Page 7427)
Specifically, this criterion would: (1) Enable the export of EHI for a single patient upon a valid request from that patient or a user on the patient's behalf

MGMA Response

In today's healthcare environment, the flow of information that most commonly occurs is when a patient requests information from a provider or when a provider transmits information to another provider. In the first instance, patients will typically approach a member of the practice's administrative staff and request their information. The two most common requests are for either a specific piece of information (i.e., their most recent blood test result) or their complete medical record. Similarly, when providers are sharing patient information with another provider, the information will most often either be specific to a test, health issue, or date of service, or (much less often) the complete medical record.

These patient and provider scenarios are critical as they intersect with both the definition of EHI and the information that must flow to avoid a charge of information blocking. Under this Proposed Rule, should a patient request their "health record" from a practice, it could trigger a requirement to collect and send an enormous amount of data, much of which would not be relevant to the patient, nor would the majority of it be clinically actionable.

This issue would also apply when the practice has received a request from another healthcare entity such as a referred to practice or long-term care facility. Under this proposal, we are concerned that the requesting entity would receive patient information that would not be relevant to the care they would be delivering. In fact, receiving voluminous amounts of data could actually impede the entity's ability to deliver care and result in a significant administrative burden by forcing them to sift through years of irrelevant data to identity the information they require to

appropriately care for the patient. In these instances, too much data can be as or more harmful than too little data.

When individuals, or entities acting on their behalf, contact their physician practice requesting information related to the care they have received, it is critical that the requirement on the practice to produce the information be balanced with the challenge in producing it. As there are serious potential consequences for practices deemed to have blocked information, minimizing the challenges associated with producing the requested information is critical if the patient is to receive the information they need. With this as the foundation, we recommend ONC adopt a tiered approach to the scope of EHI to be provided to the requesting individual.

- Tier One: ONC should establish the first tier of requested information be that specific EHI requested by the individual and that ONC encourage the individual and the producing entity to engage in a discussion with the goal of determining what EHI the individual requires. For example, the individual may ask the practice for a copy of their medical record but following a brief discussion with practice staff establish that they wish only to receive their last three laboratory test results.

  This approach allows the patient to receive exactly what they needed, with reduced administrative burden on the practice. In this example, the practice would only be deemed to be information blocking if they refused to supply the three laboratory test results.

- Tier Two: ONC should establish that when a patient requests their entire medical record, the producing entity should be required to produce the complete designated record set, as defined by the Office for Civil Rights. This would not include information related to the past or future payment for medical services. In this example, the practice would only be deemed to be information blocking if they refused to supply the designated record set.

- Tier Three: ONC should establish that when a patient requests their entire medical record and/or information related to the past or future payment for medical services, the producing entity should be required to produce the complete designated record set and/or information limited to the past payment for medical services (if the payment data was feasible and reasonable to produce). This would not include information related to the future payment for medical services. In this example, the practice would only be deemed to be information blocking if they refused to supply the designated record set and/or information related to the past payment for medical services.

  In recognition that payment information may be stored in another physical location or maintained by a business associate of the producing entity, should the request include information related to the past or future payment for medical services, the producing entity should be given an additional 30 days beyond what is the time that is generally permitted for producing the designated record set to account for the extra time it may take to produce the payment information.

- Tier Four: ONC should establish the fourth tier as including scenarios wherein another healthcare covered entity requests specific EHI on behalf of an individual. For example, a specialty practice requests the last three laboratory tests for a patient from a primary care practice. In this example, the primary care practice would only be deemed to be information blocking if they refused to supply the three laboratory test results.

- Tier Five: ONC should establish that the fifth tier of requested information includes *non-specific* EHI requested by an entity who is not the individual. For example, a specialty practice requests information regarding a patient from a primary care practice. For this

type of request the primary care practice would be required to supply a complete USCDI. In this example, the primary care practice would only be deemed to be information blocking if they refused to supply a complete USCDI.

Length of Time

The Proposed Rule does not stipulate how many years of data a practice must include in its requirement to supply health information to a requesting entity. Similar to our recommended tiered approach outlined above, we urge flexibility when establishing a time period for what information must be produced before an entity is deemed to have been blocking data. We recommend the following approach:

- Tier One requests: The producing entity would clarify with the patient the precise type of information being requested, and for what time period.

- Tier Two requests: When a patient requests their entire medical record, the producing entity would supply the entire designated record set maintained by the producing entity, regardless of how many years of data would be included.

- Tier Three requests: Requests that involve information related to past payment for medical services would require the producing entity to produce a minimum of two years of payment data, if it is feasible and reasonable to produce.

- Tier Four requests: The producing entity would engage with the requesting entity to determine precisely what the requesting entity required in terms of the type of specific information and how far back in time.

- Tier Five requests: When non-specific EHI is requested by an entity who is not the individual and the producing entity would be required to supply a complete USCDI, we recommend that a minimum of two years of data be required.

Excluding De-identified Data

MGMA supports the ONC proposal to not include de-identified data in the definition of EHI and urges the agency finalize this policy. We believe that Congress's intent in the Cures Act was to encourage the flow of clinical information between systems – not to impact and potentially discourage the creation or application of de-identified data. It takes significant time and resources to develop databases of de-identified data for research, quality improvement and quality assurance purposes. Requiring practices to make the data in these databases widely available to third parties under the fee constraints established by this rule would inhibit innovation and potentially jeopardize the de-identified nature of the information (particularly statistically de-identified data) given the wider audience to the data.

Removal of Randomized Surveillance Requirements

ONC Proposal (Page 7434)

We propose to revise § 170.556(c) by changing the requirement that ONC– ACBs must conduct in-the-field, randomized surveillance to specify that ONC–ACBs may conduct in-the- field, randomized surveillance. We further propose to remove § 170.556(c)(2), which specifies that ONC–ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year. We also propose to remove the requirements in § 170.556(c)(5) regarding the

exclusion and exhaustion of selected locations for randomized surveillance. Additionally, we propose to remove the requirements in § 170.556(c)(6) regarding the consecutive selection of certified health IT for randomized surveillance.

MGMA Response

We oppose the proposal to reduce oversight of EHR products. Decreasing the level of surveillance of EHR products sends the wrong message to both EHR developers and physician practices. For vendors, it largely removes the concern that ONC-ACBs will select them for an in-the-field randomized test of their capabilities. As it is highly unlikely that their provider clients will have the ability to discern if the vendor's product does not meet ONC certification requirements, vendors could take a lackadaisical approach to satisfying mandated criteria.

For practices, a lack of ONC oversight creates additional uncertainty as to software purchasing options. Simply put, knowing that there is the potential of in-the- field, randomized surveillance of a vendor's product will put additional pressure on vendors to produce and maintain required functionalities.

2015 Edition Certification Criteria and Standards

ONC Proposal (Page 7436)

We propose the removal of certain certification criteria from the 2015 Edition that are included in the 2015 Edition Base EHR definition.

- *We propose to remove the 2015 Edition ''problem list'' certification criterion (§ 170.315(a)(6)).*
- *We propose to remove the 2015 Edition ''medication allergy list'' certification criterion (§ 170.315(a)(8)).*
- *We propose to remove the 2015 Edition ''smoking status'' criterion (§ 170.315(a)(11)),*
- *We propose, however, to remove the requirement to code smoking status according to the adopted eight smoking status SNOMED CT® codes as referenced in the value set in § 170.207(h)*
- *We propose to remove the 2015 Edition ''drug formulary and preferred drug list checks'' criterion in § 170.315(a)(10)*
- *We propose to remove the 2015 Edition ''secure messaging'' criterion (§ 170.315(e)(2)).*

MGMA Response

We support the ONC proposal to remove certain certification criteria from the 2015 Edition that are included in the 2015 Edition Base EHR definition.

ONC Proposal (Page 7439)

This rule proposes to update the 2015 Edition by revising and adding certification criteria that would establish the capabilities and related standards and implementation specifications for the certification of health IT.

MGMA Response

Since the advent of the CMS Meaningful Use Program, ONC has created three separate certification editions, 2011, 2014, and 2015. Each edition has had an increasingly complex and comprehensive set of certification requirements, which impacts practitioners and group practices as they are typically required to adopt the latest version in order to fully participate in CMS's

particular iteration of its quality reporting programs. Delineating a specific edition of certification permits practices to establish, through their purchasing contract with their EHR vendor, that the practice software would meet the specific program requirements.

With this proposal, ONC has augmented the current certification requirements, adding significant new functionalities and capabilities. However, the certification edition for the software has remained the same-=: 2015. This nomenclature of EHR certification standards generates unnecessary confusion as eligible clinicians and groups seek to meet the various 2020 and 2021 CMS program requirements, smaller practices especially will be hamstrung by not knowing if their particular 2015 edition CEHRT meets the reporting program requirements. We urge ONC to rename the revised 2015 edition the "2020" edition to permit practices to clearly delineate in their vendor contracts which edition the vendor will support and when.

USCDI 2015 Edition Certification Criteria

ONC Proposal (page 7441)

We propose to adopt the USCDI Version 1 (USCDI v1) in § 170.213. 15 The USCDI is a standardized set of health data classes and constituent data elements that would be required to support nationwide electronic health information exchange.

MGMA Response

We support the adoption of the USCDI Version 1 as we believe it contains a more complete picture of a patient's health than the previous edition of the USCDI and will provide additional valuable information during the information exchange process.

We also urge ONC to consider adding the following element from the proposed Pediatric criteria to the USCDI core set of data elements: Recommendation 10: Flag Special Health Care Needs (page 7609). The ONC description for this recommendation states:

- "The system shall support the ability of providers to flag and un-flag individuals with special health care needs or complex conditions who may benefit from care management, decision support, and care planning, and shall support reporting."

We assert that including this data element into the USCDI would be beneficial to physician practices that furnish care management and other services.

In particular, having the ability to identify patients requiring more intensive care management in the EHR will be beneficial to furnishing care that is value-based, high-quality, and patient-centric, and has the potential to drive down health costs be enabling clinicians to deliver appropriate interventions such as preventing high-cost admissions for vulnerable patient populations.

ONC Proposal (Page 7495)

Accordingly, we propose that successful real world testing means for the purpose of this Condition of Certification that: The certified health IT continues to be compliant to the certification criteria to which it is certified, including the required technical standards and vocabulary codes sets; The certified health IT is exchanging electronic health information in the care and practice settings for which it is intended for use; and Electronic health information is received by and used in the certified health IT. We propose to limit the applicability of this Condition of Certification to health IT developers with Health IT Modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange, which are: The care coordination criteria in

§170.315(b); The clinical quality measures (CQMs) criteria in §170.315(c)(1) through (c)(3); The ''view, download, and transmit to 3rd party'' criterion in §170.315(e)(1); The public health criteria in §170.315(f); The application programming interface criteria in §170.315(g)(7) through (g)(11); and The transport methods and other protocols criteria in §170.315(h).

MGMA Response

While physician practices have adopted EHRs in record numbers over the past ten years, there is considerable and growing concern regarding the quality and usability of the software, and that EHR issues may be contributing to physician burn-out and impacting patient safety. We strongly support the inclusion of a robust process of real-world software testing. Laboratory testing has its merits, primarily the ease and speed of review and lower costs for both the software developer and the Administration. However, the ultimate goal of certification standards should be to identify products that aid physicians in real world settings while furnishing clinical care, rather than simply determining if software meets fundamental ONC criteria.

The objective of real-world testing is to verify the extent to which certified health IT deployed in operational production settings is demonstrating continued compliance to certification criteria and functioning with the intended use cases as part of the overall maintenance of a health IT's certification. Real-world testing should ensure certified health IT is capable of sharing EHI with other systems. Real-world testing should also assess that the certified health IT is meeting the intended use case(s) of the certification criteria to which it is certified within the workflow, health IT architecture, and care/practice setting in which the health IT is implemented.

ONC Proposal (Page 7446)

First, we propose that health IT certified to this criterion would have to enable the export of EHI for a single patient upon a valid request from that patient or a user on the patient's behalf.

MGMA Response

While we agree that health IT certification should include the requirement for software to export EHI for a single patient, we urge ONC to be cautious in how this policy is operationalized. 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 if notice is provided to the patient. These time periods for responding to patient record requests was established in an effort to strike an appropriate balance between providing timely responses to patient information requests and fairness to the practice producing the information.

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

- PHI is 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 is 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 quality data that has not been deidentified, while others may have electronic data stored in systems that

are strictly for performing revenue cycle functions. Additional staff time would be required to compile the complete designated record set to fulfill a patient request.

Even if a practice has migrated to an EHR, it is unlikely that they have scanned every patient record into an electronic format. Many EHRs, for example, contain only the last few years of patient records. Older paper records are typically secured either in a designated area of the practice or stored offsite. Since these older records would be considered part of the designated record set, they would need to be included in a complete medical record as requested by a patient. Assembling these records would require considerable staff time, particularly if the patient requested they be provided electronically, which would entail scanning potentially hundreds of pages of medical records.

- Form and format can be requested. Patients have the right to request that records be produced 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.

- Physicians are permitted to review 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 could be harmful to either the patient or another individual. This process requires sufficient time to both compile the complete record and conduct a sufficient review to ensure patient safety.

ONC should recognize that while some individual access requests can be relatively easy to fulfill (e.g., those that can be satisfied through the use of CEHRT), 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.

While the Privacy Rule is intended to set the outer time limits for providing access, it may 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. Further, it is typical that practices seek to meet these requests in a timely manner, well in advance of the full 30-day time period. 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 if that is feasible).

MGMA recommends ONC, in coordination with the Office for Civil Rights (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 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 their rights under HIPAA regarding access to their medical record (or a specific component of the record), including that they can request that the record be provided in a specific time frame and format. This campaign could emphasize that practices should provide the record as quickly as possible and encourage that clinicians discuss the request with the patient to determine if they want the entire medical record or just specific information contained in the record.

- Recognize that many practices now employ a patient portal that permits the patient to retrieve significant portions of their designated record set automatically online. While the portal may not capture, for example, older records created prior to the practice adopting its EHR, a patient portal may have the information needed by the patient, such as recent lab results, medications, allergies, etc more readily available. 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 seven 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 two business days of the information being available to the eligible professional. The five additional days would assist those practices who have patient portals but who do not use 2015 Edition CEHRT.

ONC Proposal (Page 7447)

Second, this criterion would support the export of EHI when a health care provider chooses to transition or migrate information to another health IT system.

MGMA Response

We strongly support this proposal. One of the challenges practices face involves replacing EHR software that does not meet clinical and administrative needs, has been de-certified by ONC, or is in some other way unsuitable for their organization. As EHR vendors rarely permit patient data to be transferred from one product to another in a structured format, replacing software often entails printing and scanning patient records into a PDF format.

Standardizing the format in which the vendor must produce patient information will be critical to its export applicability and success. Requiring vendors to export EHI in a standardized structured format would not only make the transition to a new product less administratively onerous for the practice but would significantly decrease the likelihood of a patient safety issue arising from a clinician's lack of access to accurate data. For this information to be useful for practices, we believe that ONC should require the capability to permit practices to request time-delineated exports. Additionally, the image types that should be shared should include, at a minimum, .jpeg, .jpg, .png, .gif, .pdf, .bmp. We also believe there would be value in requiring developers make clear the types of EHI they cannot support when they provide their export format documentation.

While ONC has not specified a content standard for the EHI export, we believe it is critical to require that developers provide the format for the exported EHI (e.g., data dictionary, export support file). Requiring the developer's export format to be made available via a hyperlink is also appropriate. For system transition use cases in which a physician is moving to a new health record system, we support the ONC directive that would require that Health IT developers reasonably cooperate and assist. Further, knowing that data can be exported without undue

burden to a competitor's product may act as catalyst for improved vendor product support and certification adherence.

ONC Proposal (Page 7429)

The Cures Act adds a new Condition and Maintenance of Certification requirement that health IT developers successfully test the real world use of the technology for interoperability in the type of setting in which such technology would be marketed.

MGMA Response

Many clinicians practice in solo or small group practices that are independent of larger hospital or health systems and have limited resources to vet and compare EHR products for their capabilities and usability. Implementing an EHR system is a significant capital and human resource investment for a practice. Therefore, physicians should have the assurance that the system they are purchasing will meet their clinical and administrative requirements. We urge ONC to finalize this proposal.

ONC Proposal (p. 7459)

Pediatric Certification Criteria

These include eight recommendations related to the Priority List: Recommendation 1: Use biometric specific norms for growth curves and support growth charts for children. Recommendation 2: Compute weight-based drug dosage. Recommendation 3: Ability to document all guardians and caregivers. Recommendation 4: Segmented access to information. Recommendation 5: Synchronize immunization histories with registries. Recommendation 6: Age- and weight-specific single-dose range checking. Recommendation 7: Transferrable access authority. Recommendation 8: Associate maternal health information and demographics with newborn. We also developed two additional recommendations beyond the Priority List which relate to other items within the Children's Format that are considered important to pediatric stakeholders. These additional recommendations, which we believe may be supported by certified health IT, are as follows: Recommendation 9: Track incomplete preventative care opportunities. Recommendation 10: Flag special health care needs.

MGMA Response

We support the development of a pediatric-specific EHR certification program and applaud ONC's proposal to implement section 4001 of the Cures Act by creating new criteria for health IT used in the care of children. The ten proposed recommended clinical priorities—selected after discussions with from pediatric experts—represent a positive step forward for improving EHRs used in the care of children. These priorities and their technical worksheets will provide an opportunity to address safety and usability in pediatric settings. We offer the following recommendations to help ensure that the pediatric certification program will meet the needs of clinicians delivering care to children:

- Release Guidance to Support the Priority Areas. We urge ONC to develop specific and detailed guidance/implementation specifications for each of the ten proposed pediatric clinical priorities. We believe that the release of pediatric-specific certification criteria guidance will provide much needed information to help guide implementation.

- Leverage Pediatric and Usability Experts**.** As the agency did in identifying the ten priority areas, we recommend ONC engage with pediatric care experts to draft the implementation guides and test procedures. Specifically, ONC should involve pediatricians, pediatric

nurses, and safety, usability, and human factors experts in the development process.

- Require All Ten Priorities for Certification**.** In order to ensure that this certification process is supportive of pediatric care and will lead to measurable improvement in the care delivery process, we recommend that the certification of any EHR product used in the care of children require the inclusion of all ten clinical priorities.

Improved Mapping of CEHRT to Pediatrics

In the Proposed Rule, ONC aligns the technical worksheets for each of the 10-recommended clinical priorities with their corresponding certification criteria from ONC's 2015 edition and changes made to the criteria through these regulations. ONC should extend the approach of mapping criteria from the 2015 edition to other aspects of the pediatric-focused criteria.

- Require Pediatric-focused Test Scenarios**.** EHR developers are required to employ testing scenarios to establish that they are in compliance with the 2015 Edition requirements. These testing scenarios mirror real-world encounters to evaluate whether the system can meet ONC's criteria. For the pediatric certification, ONC should require that some of the testing scenarios used be vendors should involve pediatric patients and pediatric-specific factors.

- Leverage Pediatric End-Users**.** To receive certification for a health IT product, the 2015 Edition requires testing from at least 10 end users (such as physicians or nurses). In recognition of the unique aspects of pediatric care, ONC should require that pediatric clinicians participate in end-user testing for those entities that are seeking pediatric-focused certification for their system. For pediatric-focused certification, we recommend that a minimum of five of the end-user testers be clinicians that care for pediatric patients**.**

- Require Use of Pediatric Test Data. EHR developers use data in test cases to demonstrate that their products meet ONC's certification requirements. For a pediatric-focused certification, ONC should supply test data for mock pediatric patients and require that the test data must involve mock data of children.

ONC Proposal (Page 7466)

We propose that, as a complementary Condition of Certification, health IT developers of certified health IT must provide an assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes. More specifically, developers would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Such actions may inhibit the appropriate access, exchange, or use of EHI and are therefore contrary to this proposed Condition of Certification and the statutory provision that it implements.

MGMA Response

We support the ONC proposal to require, as a Condition of Certification, that health IT developers provide an assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes. We agree that these developers should be prohibited from taking any action that could interfere with the ability of a practice to access or use certified capabilities for any purpose within the scope of the technology's certification.

We are concerned, however, that earlier in this proposal the agency outlined its plan to scale back randomized surveillance of EHR products. We do not believe that the only method for ensuring that developers are implementing product capabilities for their intended purposes is end-user reporting. Often practices do not have the technical expertise to determine if their vendor has not implemented a feature of the software in the appropriate manner. Again, we strongly recommend that ONC deploy randomized surveillance as a deterrent to and to ensure EHR software meets the needs of clinicians and does not pose a safety hazard to patients.

ONC Proposal (Page 7466)

We propose, as a Condition of Certification requirement, that a health IT developer that produces and electronically manages EHI must certify health IT to the 2015 Edition ''electronic health information export'' certification criterion in § 170.315(b)(10)

MGMA Response

We support ONC's proposal to require that health IT developers that produce and electronically manage EHI must certify health IT to the 2015 Edition ''electronic health information export'' certification criterion.

ONC Proposal (Page 7476)

As a Condition of Certification (and Maintenance thereof) under the Program, the Cures Act requires health IT developers to publish APIs that allow ''health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law.'

MGMA Response

The Proposed Rule would require developers of certified health IT to share EHI with third-party applications of a patient's choice through new, innovative APIs that utilize the FHIR protocol. These third-party application developers, which are entering the healthcare market at a rapid pace, are typically not required to abide by the provisions in HIPAA due to the fact they offer their applications directly to consumers and not on behalf of covered entities such as providers or health plans. It is imperative that ONC develop an approach for how practices and other entities that are, for the most part, covered entities or business associates under HIPAA, share EHI with these non-HIPAA entities, and ensure that such third-party applications are equipped to securely handle sensitive patient information.

We are concerned that patients will not have adequate information to be educated consumers and may not fully comprehend that they are assuming the risk of the security practices implemented by their chosen application. Consumers do not necessarily understand when their information is and is not protected by HIPAA. While we appreciate OCR's recently released guidance clarifying that healthcare providers are not responsible under the HIPAA Security Rule for verifying the security of a patient's chosen third party application, this "safe harbor" does not address the potential vulnerability of patient information when sent to the application.

The Proposed Rule stipulates that a practice is not permitted to conduct "verification" checks on individual third-party applications before allowing the application to connect to its API, but rather must conduct such "verification" on the developers themselves and must complete the process within five business days. Although ONC provides some examples of acceptable "verification" processes in the Proposed Rule, the permissible scope and purpose of "verification" is still unclear given that a practice is prohibited from seeking additional information about the third-party developer's application or its security readiness. It is imperative that ONC provide further guidance on the types of "verification" that will be permitted and permit practices to undertake

some form of review of third-party applications themselves before permitting them to connect to their APIs.

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

We have significant concerns regarding the complex and costly compliance requirements on practices and the documentation, patient education and risk issues related to the proposed API provisions. Simply put, the traditional approach to granting permission to APIs may be insufficient. According to the ONC Proposed Rule: "APIs should require a "yes" attestation by the app that patients are provided meaningful notice and control over how their protected health information (PHI) is used to connect to the API." This traditional requirement for the user to click "yes to continue" or "I accept" to the conditions type of model will not be sufficient to appropriately communicate to the patient the risk managing that data might have or to give confidence to providers concerned that patients understand the risks and benefits of this data use. It is imperative that patients fully comprehend the risk prior to using their data in apps and in choosing using the API.

Permitted Fees

ONC Proposal (Page 7470)

We propose that protected communications include, but are not limited to: • The costs charged by a developer for products or services that support the exchange of electronic health information (e.g., interface costs, API licensing fees and royalties, maintenance and subscription fees, transaction or usage-based costs for exchanging information); the timeframes and terms on which developers will or will not enable connections and facilitate exchange with other technologies, individuals, or entities, including other health IT developers, exchanges, and networks; • the developer's approach to participation in health information exchanges and/or networks; • the developer's licensing practices and terms as it relates to making available APIs and other aspects of its technology that enable the development and deployment of interoperable products and services; and • the developer's approach to creating interfaces with third-party products or services, including whether connections are treated as ''one off'' customizations, or whether similar types of connections can be implemented at a reduced cost. Importantly, we further propose that information regarding business practices related to exchanging electronic health information would include information about the switching costs imposed by a developer, as we are aware that the cost of switching health IT is a significant factor impacting health care providers adopting the most exchange-friendly health IT products that are available.

MGMA Response

In the Proposed Rule, ONC requires that generally health IT vendors are to make information exchange through APIs available at no cost. However, the Proposed Rule does permit API Technology Suppliers to charge practices fees for upgrades related to APIs. However, the rule fails to establish specific parameters on what would constitutes an "upgrade" or how much the vendor-imposed fee could be.

Given this flexibility, we are concerned that API Technology Suppliers could use the ONC requirement to make data available via API as an excuse to increase the base price of the system

for all users, regardless of whether they are using the API features. By proposing to allow vendors to charge their users for system upgrades, we are concerned that ONC is providing an exception for vendors to continue to engage in practices that could stifle interoperability. We anticipate that EHR vendors will pass on the cost of complying with these regulations to practices through either excessive fees or mask the fees and simply increase the purchase cost of the EHR systems themselves.

While we welcome ONC outlining a general prohibition against "unreasonable" fees associated with APIs, we continue to be concerned that EHR software vendors will use the fees permitted under the rule as an opportunity to unfairly charge physician practices or leverage "permitted" fees to avoid offering true interoperability between external systems or applications.

We recommend the creation of a tiered structure for fees charged to practices for APIs. ONC should consider the following categories where the specific requirements of the technology define the fees practices would be required to pay:

- Zero fee. In this category, the practice could not be charged by an API Technology Supplier for an API used in support of data exchange in compliance with federal requirements (e.g., costs associated with health information exchange, patient access, reporting quality measures, and data segmentation for privacy).
- Cost Only fee. In this category, an API Technology Supplier would be permitted to charge a practice the cost of interfacing APIs with a non-API Technology Supplier's commercial technology (e.g., commercial lab systems, commercial picture archiving and communication systems, commercial data analytics services).
- Cost Plus a Reasonable Profit. In this category, an API Technology Supplier would be permitted to charge a practice their cost plus a "reasonable" profit when implementing practice-approved custom API development or creating practice-approved custom apps (e.g., creating proprietary mappings for technology unique to a health system or establishing connections with non-commercially available technology.)

In general, we urge that API Technology Suppliers be prohibited from implementing technology in non-standard formats with the intent of adding unnecessary complexity and fees for practices. We assert that ONC should finalize a fee structure, that while being fair to API Technology Suppliers, increases fee transparency and facilities more technology purchasing decisions by practices.

ONC Proposal

…we propose in § 170.404(a)(3)(i)(B)(1) that in order to be a permitted fee, a fee imposed by an API Technology Supplier must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. This would require an API Technology Supplier to apply fee criteria that, among other things, would lead an API Technology Supplier to come to the same conclusion with respect to the permitted fee's amount each time it interacted with a class of persons or responded to a request. Accordingly, the fee could not be based on the API Technology Supplier's subjective judgement or discretion.

MGMA Response

The area of permissible fees is a challenging one. While we appreciate the requirement in the Proposed Rule that any fee imposed by an API Technology Supplier must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated

classes of persons and requests, we remained concerned that vendors may not apply this uniformly.

Currently, the CMS QPP program requires eligible clinicians and group to employ 2015 CEHRT in order to score points in the Promoting Interoperability component of MIPS or an Advanced Payment Model. We are hearing from our members that a significant number of them may not be upgrading from 2014 CEHRT due to the financial burden of the upgrade and/or the burdensome implementation process. As well, other practices are reporting that their current vendor has not produced a 2015 Edition version of the software and switching EHR vendors is cost-prohibitive. Adding significant new functionality and certification requirements for EHR developers will inevitably drive up software costs for physician practices. ONC should seek to minimize these costs by imposing strict guidelines on the fees that EHR developers are permitted to charge practices for API deployment.

ONC Proposal (Page 7488)

Moreover, in order to be permitted, the fee must not be based in any part on whether the API User is a competitor or potential competitor, or on whether the API Data Provider or API User will be using the data accessed via the API technology in a way that facilitates competition with the API Technology Supplier…Second, we propose in § 170.404(a)(3)(i)(B)(2) that in order to be a permitted fee, a fee imposed by an API Technology Supplier must be reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting the API technology to, or at the request of, the API Data Provider to whom the fee is charged. Third, we propose in § 170.404(a)(3)(i)(B)(3) to require that in order to be a permitted fee, the costs of supplying, and if applicable, supporting the API technology upon which the fee is based must be reasonably allocated among all customers to whom the API technology is supplied or for whom it is supported. Last, we propose in § 170.404(a)(3)(i)(B)(4) to require that in order to be a permitted fee, the API Technology Supplier must ensure that fees are not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier.

MGMA Response

We support the requirement in the Proposed Rule that the fee must not be based in any part on whether the API User is a competitor or potential competitor, or on whether the API Data Provider or API User will be using the data accessed via the API technology in a way that facilitates competition with the API Technology Supplier.

We support the requirement in the Proposed Rule that any fee imposed by an API Technology Supplier must be reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting the API technology to, or at the request of, the API Data Provider to whom the fee is charged.

ONC Proposal (Page 7488)

In § 170.404(a)(3)(ii), we propose to permit an API Technology Supplier to charge API Data Providers reasonable fees for developing, deploying, and upgrading API technology. Fees for ''developing'' API technology comprise the API Technology Supplier's costs of designing, developing, and testing API technology to specifications that fulfill the requirements of the API-focused certification criteria adopted or proposed for adoption at 45 CFR 170.315(g)(7) through (g)(11). Fees for developing API technology must not include the API Technology Supplier's costs of updating the non-API related capabilities of the API Technology Supplier's existing health IT, including its databases, as part of its development of the API technology. These costs would be

connected to past business decisions made by the API Technology Supplier and typically arise due to health IT being designed or implemented in nonstandard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI.

MGMA Response

We appreciate that ONC has sought to limit the fees that API Technology Suppliers can charge API Data Providers. However, we believe the proposed approach of limiting what the vendor can charge the provider to those fees that "reasonable" for "developing, deploying, and upgrading API technology" is inadequate and will lead to practices being forced to incur significant costs that could impact their ability to implement the technology.

The challenge when relying on the term "reasonable" is that interpretation of what fees are estimated to be reasonable is left up to the entity who is to receive the fees. The potential costs associated with technology are significant and will inevitably be passed on to practices. ONC will need to be vigilant in ensuring that software vendors do not engage in unfair business practices. We recommend that the agency release additional guidance specific to the permissible fees issue, conduct educational webinars on this topic, and establish a toll-free number and email/website-based complaint process where providers can lodge fee-based complaints. Vendors found to be engaging in unfair business practices should have to pay restitution to the harmed practices, incur a fine, and/or have their certification revoked. This approach would act as a clear deterrent to vendors imposing unreasonable fees.

ONC Proposal (Page 7488)

In § 170.404(a)(3)(iv) we propose to permit an API Technology Supplier to charge fees to API Users 92 for value added services supplied in connection with software that can interact with the API technology. These ''value-added services'' would need to be provided in connection with and supplemental to the development, testing, and deployment of software applications that interact with API technology. Critically, fees would not be permitted if they interfere with an API User's ability to efficiently and effectively develop and deploy production-ready software.

MGMA Response

While we agree that vendors should be permitted to charge fees for mutually-agreed upon "value-added" services, we strongly urge the agency to not require that providers accept these value-added services.

ONC Proposal (Page 7472)

We propose that where a communication relates to subject areas enumerated in § 170.403(a)(1) and there are federal, state, or local laws that would require the disclosure of information related to health IT, developers must not prohibit or restrict in any way protected communications made in compliance with those laws.

MGMA Response

We support the proposal that health IT developers must not prohibit or restrict in any way protected communications made in compliance with federal, state, or local laws. We urge the agency to include this issue in guidance and provider education efforts.

ONC Proposal (Page 7472)

We propose that if health IT developers were to impose prohibitions or restrictions on the ability of any person or entity to communicate information about cybersecurity threats and incidents to government agencies, such conduct would not comply with this Condition of Certification.

MGMA Response

We agree that if health IT developers were to impose prohibitions or restrictions on the ability of any person or entity to communicate information about cybersecurity threats and incidents to government agencies, such conduct should not comply with this Condition of Certification. Cyberattacks against physician practices are on the increase and they represent a significant threat not only to the practice as a business, but also to the organization's ability to safely treat their patients.

ONC Proposal (page 7473)

We propose that the benefits to the public and to users of health IT of communicating information about a health IT developer's failure to comply with a Condition of Certification or other Program requirement (45 CFR part 170) justify prohibiting developers of health IT from placing any restrictions on such protected communications. Information regarding the failure of a health IT product to meet any Condition of Certification or other Program requirement is vital to the effective performance and integrity of the Program, which certifies that health IT functions consistent with its certification.

MGMA Response

We strongly concur with this proposal. ONC must establish an environment where practices are not only comfortable in coming forward to report usability, patient safety, or software functionality issues with their EHR products but actually encouraged to do so. ONC should consider developing a patient safety-focused reporting system that would permit end-users to report issues with software that could or did lead to harm to the patient. Implementing this type of issue reporting program and subsequent transparency policy will increase provider and patient confidence in EHR products and put health IT developers on notice that they must be vigilant in producing high quality software.

ONC Proposal (Page 7476)

We propose that a health IT developer must notify all customers and those with which it has contracts/agreements, within six months of the effective date of a subsequent final rule for this Proposed Rule, that any communication or contract/agreement provision that contravenes this Condition of Certification will not be enforced by the health IT developer.

MGMA Response

MGMA supports the agency proposal that a health IT developer notify all their practice customers, within six months of the effective date of the final rule, that any communication or contract/agreement provision that contravenes this Condition of Certification will not be enforced by the health IT developer. We also support the proposal that this notice be provided annually up to and until the health IT developer amends the contract or agreement to remove or void any contractual provision that contravenes this Condition of Certification.

Further, while we agree that, as a Maintenance of Certification requirement, health IT developers must amend their contracts or agreements to remove or void any provisions that contravene the

Condition of Certification within a reasonable period of time, we urge ONC to stipulate that this timer period be no more than one year from the effective date of the final rule.

ONC Proposal (Page 7478)

Given FHIR Release 4's public release and that the industry will begin to implement Release 4 in parallel with this rulemaking, we request comment on the following options we could pursue for a final rule.

MGMA Response

MGMA supports FHIR Release 4 as the standard health IT developers would be required to certify to.

Information Blocking

In general, we recommend ONC review the very broad definitions of healthcare "actors" and information blocking, with particular emphasis on the definitions of health information networks and health information exchanges. We are also concerned about the challenge practices will face seeking to comply with these information blocking provisions, in particular the documentation requirements.

Further, there is insufficient flexibility built in to both the EHI definition and the definition of what would constitute information blocking. If, for example, a practice was to produce 99 percent of the requested EHI, would they be deemed to have blocked information? We assert that the broader the definition of EHI, the more flexibility should be afforded the entity producing the EHI.

ONC Proposal (Page 7593)

Intellectual property. A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's health IT (including third-party rights), provided that— (1) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and (2) A health IT developer does not prohibit the communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section. (D) Screenshots. A health IT developer may require persons who communicate screenshots to— (1) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with §170.403(a)(2)(ii)(D)(3) or to conceal protected health information; (2) Not infringe the intellectual property rights of any third parties, provided that— (i) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification; (ii) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work;

MGMA Response

The Cures Act incorporated privacy and security issues when directing HHS to develop the strategy of removing health IT vendor-imposed "gag clauses" on practices communicating health IT issues to the government. While we understand, from the perspective of health IT developers, the importance of protecting intellectual property, banning practice use of screen shots in support of their case should not be permitted. The more appropriate approach would be for practices to be prohibited from sharing what is deemed by ONC to be screen shots containing intellectual

property with any entity other than ONC and for ONC to guarantee to the health IT developers that the confidentiality of their intellectual property would be maintained.

We also recommend the following:

- ONC should require that any person or organization who makes a communication to ONC that includes screen shots not be subject to retaliatory action from the health IT vendor which could reasonably be considered was due to their whistleblowing activity;

- ONC should stipulate that a health IT developer cannot prohibit the fair use communication of screenshots of the developer's health IT, subject to limited restrictions;

- ONC can prohibit the altering of screenshots, except to annotate the screenshot, resize it, or to redact a screenshot or to conceal protected health information; and

- ONC should prohibit the infringement of the intellectual property rights of any third parties, provided that the health IT developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification.

ONC Proposal (Page 7493)

Relatedly, in § 170.404(a)(4)(ii)(B) we propose to prohibit an API Technology Supplier from imposing any collateral terms or agreements that could interfere with or lead to special effort in the use of API technology for any of the above purposes.

MGMA Response

We concur with the agency's proposal to prohibit an API Technology Supplier from imposing any collateral terms or agreements that could interfere with or lead to special effort in the use of API technology for any of the stated purposes.

ONC Proposal (Page 7523)

We propose to establish an exception to the information blocking provision for practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.

MGMA Response

We agree with the ONC inclusion of the "Exception – Preventing Harm" blocking exception. Those engaged in the access, exchange, and use of EHI must be assured that practices/policies that prevent harm will not interpreted as stifling interoperability. Including an exception to prevent the wrong data from being shared is important but ONC should also recognize the issue of technical data corruption and/or incorrect patient data (due to patient matching errors) when finalizing this policy. (If data corruption results in the infeasibility or downtime of the system, we would recommend deferring to those exceptions.)

The inclusion of an opportunity for clinicians to explain why information sharing may result in harm is particularly salient in cases related to adolescent medicine, behavioral health, infectious diseases, substance abuse, and others where complexities of local policies, state law and existing federal law about the role of the clinician in determining what information may be withheld in the

patient's (or another person's) best interest. The reasons for not sharing information under this exception of harm should be left to the professional judgement of the clinician and can be documented within the EHR. The documentation can include the reasoning and conditions applied and must be made available for other users of the system and the patient to ensure that this exception does not result in unintended consequences. It is recognized that this will require implementation activities from health IT vendors, and thus should be reflected in the enforcement timeline for the final rule.

As ONC acknowledges, regulations such as 42 CFR Part 2, or the self-pay test provision in HITECH require patient consent prior to sharing, yet the agency contends that the exemption cannot be justified just because a patient did not provide consent to share this data. This of course would result in the transmitted record being incomplete. As it moves to finalize this policy, ONC should take into account the fact that many EHRs do not have the capability to appropriately segregate sensitive data from other portions of the record.

Until EHR software has evolved to the point where sensitive data can be easily segmented, and regulations such as 42 CFR Part 2 are fully aligned with HIPAA, practices will experience challenges outside their control related to sharing records containing sensitive health information. Further, as Congress and the Administration are reviewing the issues around aligning 42 CFR Part 2 with HIPAA, we note that the information blocking rule clearly does not supersede 42 CFR Part 2 rules. We recommend ONC delay finalization of this component of the regulation until final disposition of 42 CFR Part 2.

ONC Proposal (Page 7526)

We propose to establish an exception to the information blocking provision for practices that are reasonable and necessary to protect the privacy of an individual's EHI, provided certain conditions are met.

MGMA Response

We concur with the agency that legitimate privacy concerns should be the basis for an exception to the information blocking provision. If ONC is truly to be patient-centric and respect the wishes of patients when it comes to data sharing, we urge the agency to modify this data blocking exception category. This regulation appears to assume that the vast majority of patients wish their health information to be released by their physician to third-parties who are not bound by HIPAA Privacy and Security regulations. While this may be the case for some patients, we contend that others would prefer that the practice continue to restrict access to third parties, primarily in cases that do not include sharing of information for treatment or payment purposes.

In today's physician practice environment, practice staff and patients typically engage in a conversation regarding the patient's health information. In addition to providing the patient the organization's Notice of Privacy Policies and addressing any questions the patient may have regarding the contents of that document, the patient may request specific restrictions to disclosures. For example, they may have a relative, neighbor, or acquaintance who is a staff member of the practice and they may request that this individual not be provided access to the patient's health information. If this can reasonably by accomplished, the practice will agree to this stipulation. In addition, the patient, having agreed to pay out-of-pocket and in full, may request that the bill for a test or procedure not be submitted to their insurance for payment. By law, the practice must adhere to that request.

There are other cases where, due to the sensitive nature of the health information, the patient would prefer that their information be tightly controlled by the practice and released only in the case of payment or treatment (and perhaps even in treatment cases only after being specifically

authorized by the patient). It is with these cases in mind that we encourage ONC to modify the Promoting Privacy of EHI exception policy by implementing changes to the sub-exception conditions:

- The individual made the request to the actor not to have his or her EHI accessed, exchanged, or used;
- The individual's request was initiated by the individual without any improper encouragement or inducement by the actor; and
- The practice or its agent documents the request within a reasonable time period.

We recommend that the practice be permitted to ask the patient what their preference is regarding making their health information available to requesting entities. This can be accomplished by having the practice provide a form to the patient where they indicate if they would like to have their health information disclosed to third parties. To ensure that the content of this form would be absent of any "improper encouragement or inducement," we would encourage ONC, in consultation with OCR, to develop recommended language and/or a model form. Adopting this approach would place the patient in control of their health information and would permit the practice to segment those records that would not be released via an API or other method.

Further, we are concerned that given the limited nature of the sub-exceptions and stringent documentation requirements for meeting them that practices will be understandably concerned about inadvertently triggering a violation of the information blocking requirements. To avoid doing so, practices may be unintentionally incentivized to *overshare* EHI *without* satisfying privacy-protective pre-conditions established by HIPAA and other laws, such as the requirements at 42 CFR Part 2. We recommend that ONC clarify in the final rule that practices will not face penalties under the information blocking provisions when they elect to not disclose information in a good faith effort to comply with HIPAA, state privacy regulations, or other pertinent laws. While it is possible that entities may inappropriately seek to use privacy laws as a shield against disclosing EHI, the requirement that practices decline disclosures only in good faith should significantly reduce this possibility, as it is greatly outweighed by the increased privacy and security protections for individuals.

As currently defined in the Proposed Rule, the privacy exception would require significant administrative complexity to implement. For example, to meet the "pre-condition not satisfied" sub-exception, the practice not only is required to have written policies and procedures in place concerning the federal or state privacy pre-condition but must also do "all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide" a consent or authorization to share the information. This is an extremely onerous requirement and contradicts the Administration's stated intent of reducing the overall administrative burden on practices.

When an individual is directing the disclosure of his or her EHI, it is reasonable that practices engage in the level of effort provided for in this Proposed Rule to try to satisfy a privacy pre-condition. For other use cases, however, we believe that practices should be permitted to decide that it would be too burdensome to seek multiple consents or authorizations to share information at the request of a third party. For example, if a case management service requests access to EHI pertaining to multiple patients' substance use disorder treatment, the practice should not be penalized for deciding that it would be too difficult to seek consent or authorization from each applicable patient to share EHI with the case management service provider.

The solution to unlocking information protected by differing state or federal laws is to better harmonize state and federal laws to the HIPAA standard – thereby removing any preconditions to sharing the information for TPO purposes. Penalizing practices for not engaging in "all things

reasonably necessary within its control" to obtain consents or authorizations only stands to further aggravate the burdensome nature of more stringent privacy laws.

Given the current patchwork of state privacy laws, however, ONC is encouraged to adapt its proposal to permit practices who operate across multiple states to implement the pre-conditions of state laws that are the most stringent for purposes of this sub-exception. It is often too difficult for organizations operating across state lines to develop different consent workflows for each state, and ONC is correct in recognizing that practices instead will likely implement the most stringent state law.

If practices implement a state-mandated pre-condition consistently when responding to requests, we believe they should be permitted to select which portions of a state law to implement globally across states rather than being required to provide "all privacy protections afforded by that law across its entire business." ONC should give practices the flexibility to select which state law requirements they wish to apply globally as opposed to just the residents of the applicable state.

ONC affirms that any policy to protect the privacy of an individual's EHI must be consistent with applicable laws related to health information privacy, including the HIPAA Privacy Rule as applicable, as well as with other applicable laws and regulations, such as the HITECH Act, 42 CFR Part 2, and state laws. ONC further proposes that a practice would need to satisfy at least one of four proposed sub-exceptions in order to be covered by this exception:

- Pre-condition not satisfied: Not providing access, exchange, or use of EHI when a state or federal law requires that a condition be satisfied before a practice provides access, exchange, or use of EHI, and the condition is not satisfied;

- Developer not covered by HIPAA: Not providing access, exchange, or use of EHI when the actor is a health IT developer of certified health IT that is not covered by the HIPAA Privacy Rule in respect to a practice;

- Denying right to access: A covered entity, or a business associate on behalf of a covered entity, denying an individual's request for access to their electronic PHI under HIPAA; and

- Individual's request not to share: Not providing access, exchange, or use of EHI pursuant to an individual's request, in certain situations.

Practices take their responsibility to safeguard and protect the privacy of patient information with which they have been trusted very seriously. While we appreciate the detailed approach and intention behind this exception, the four sub-exceptions are overly complex, and if adopted as proposed, could create significant and unnecessary administrative complexity and burden for practices.

Recommendations:

- ONC should stipulate that practices are required to only meet existing requirements under HIPAA in order to reduce the proposed administrative complexity. At a minimum, ONC should seek to align these requirements with current HIPAA regulations.

- ONC should clarify why existing HIPAA requirements are insufficient to adequately protect patient data.

- ONC should clarify how these new privacy requirements will be integrated with the changes to HIPAA requirements expected to be released by OCR.

- ONC should provide detailed guidance on how this exception will work in a practice that (a) has facilities in several states, (b) sees patients from several states, and (c) uses telehealth services that involve vendors, patients and providers in multiple states. In the Proposed Rule, the agency indicated it is considering inclusion of an accommodation in this sub-exception that would recognize an actor's observance of a legal precondition if that actor is required by law to satisfy it in at least one state in which it operates. With HIPAA requiring that practices adhere to the most restrictive rules regarding PHI disclosures, it is unclear how "choosing" one jurisdiction to follow would comply with HIPAA.

  Complicating matters further, later in the Proposed Rule ONC states "we would also need to carefully consider how to ensure that before the use of the most stringent restriction is applied in all jurisdictions, the actor has provided all privacy protections afforded by that law across its entire business." These appear to be contradictory and will add to practice confusion regarding what information to share and when to share it.

- ONC should provide guidance detailing how practices should handle situations where certain sensitive health data fall under different federal or state regulations. Segmentation of data is a critical issue and practices will need explicit guidance to assist with compliance.

- ONC should provide guidance explaining what happens when a patient "opts out" of interoperability. For example, what does the practice do if the patient has decided they do not wish their information to be shared with the local HIE? Even more complex is the situation where the patient refuses to participate with the local HIE for only certain portions of their data.

- ONC should clarify that providers must properly document their rationale for using a sub-exception. It is proposed that practices be required to give patients the chance to consent to share information, while at the same time practices would be prohibited from encouraging patients not to share their information. Implementing this policy will be confusing to practices as under HIPAA, practices are permitted to disclose health information for purposes of TPO without patient authorization.

  ONC appears to be requiring practices to prove they presented patients a choice in whether to disclose this information. Receiving patient consent prior to TPO disclosures will result significant administrative burden and complexity for practices and could have the unintended consequence of information being disclosed inappropriately or not being disclosed when it is needed.

- ONC proposes that a practice must provide the patient with an opportunity to consent / provide authorization to share their health data. The agency requests information on the actions a practice should take within their control to provide an individual with a meaningful opportunity to provide a required consent or authorization, and whether different expectations should arise in the context of a consent versus a HIPAA authorization.

  We are concerned with requiring practices to create new policies outside of the current HIPAA policies that have been used by practices for many years and are understood by both practices and patients. Adding a "meaningful" opportunity to consent to the patient, with its requisite new forms and procedures, adds new burdens and does not appear to solve any existing problems. We would recommend leveraging existing HIPAA forms, policies and procedures. If revisions are finalized, we urge that ONC phase in these

modifications to existing HIPAA requirements and provide ample lead time for practices to make any changes to existing forms, policies, and procedures.

ONC Proposal (Page 7535)

*We propose to establish an exception to the information blocking provision that would permit actors to engage in practices that are reasonable and necessary to promote the security of EHI, subject to certain conditions***.**

MGMA Response

Security-related threats to EHI are constantly increasing, and any practice that transmits EHI must continue to exercise vigilance to ensure the security of the transmission. For this reason, we support ONC establishing an exception to the information blocking prohibition when a practice denies access to information due to a tailored, non-discriminately implemented security practice directly related to safeguarding the confidentiality, integrity and availability of EHI.

We concur with ONC when it states that robust security protections are critical to promoting patient trust and confidence--that EHI will be collected, used, and shared in a manner that protects individuals' privacy and complies with applicable legal requirements. The public must have confidence in the security of their EHI if interoperability is to be successful. The growing incidence of cyber-attacks in healthcare and other industry sectors has impacted that confidence.

ONC has provided two methods of denying access, exchange or use of EHI on security grounds: (i) on the basis of a written organizational security policy; or (ii) on a case-by-case, facts and circumstances basis. These would apply when a security practice is necessary to mitigate the security risk to EHI, and there are no reasonable and appropriate alternatives to the practice that are less likely to interfere with the access, exchange or use of EHI. While practice security policies and procedures often provide strong processes for evaluating and mitigating risks, it can be difficult in a written organizational policy and procedure to address specific parameters for establishing differing levels of access to various systems that contain EHI. As a result, we support ONC providing practices options in how they would evaluate requests on a case-by-case basis to address potential security risks.

ONC Proposal (Page 7538)

We propose to establish an exception to the information blocking provision that would permit the recovery of certain costs reasonably incurred to provide access, exchange, or use of EHI.

MGMA Response

In its definition of information blocking, ONC includes any fee that is likely to interfere with the "access, exchange, or use of EHI." ONC notes, however, that this definition "may be broader than necessary to address genuine information blocking concerns and could have unintended consequences on innovation and competition." We agree with ONC's concerns that an overly broad exception for the recovery of costs could protect rent-seeking, opportunistic fees and exclusionary practices that interfere with the access, exchange, and use of EHI.

We support the rule's provision that the method by which a vendor or other entity recovers its costs must not be based on the sales, profit, revenue, or other value derived from the access to, exchange of, or use of EHI, including the secondary use of such information that exceeds the actor's reasonable costs for providing access, exchange, or use of EHI. We are also supportive of permitting under the exception only those revenue-sharing or profit-sharing arrangements if such arrangements are designed to provide an alternative way to recover the costs reasonably incurred

for providing services. Excluding certain costs regardless of this exception makes sense, including: costs due to non-standard design or implementation choices; subjective or speculative costs; fees prohibited under the HIPAA Privacy Rule; individual electronic access; and export and portability of EHI maintained in EHR systems, so long as the vendor does not attempt to "hide" additional fees under these categories.

One issue ONC should clarify is whether clinicians who did not participate in the CMS Meaningful Use EHR Incentive Program or the QPP and who may not have certified EHRs are subject to this regulation. We believe additional consideration should be afforded for these clinicians as the costs to come into compliance with the information blocking requirements will substantial and they were not the recipients of federal incentive dollars. It is patently unfair to require practices that do not have certified systems to be subject to these requirements and on the same timeline as those practices that have certified systems. We recommend ONC develop exceptions to the information blocking requirements, at least in the near term, for clinicians who do not have certified systems.

ONC is clearly adopting a narrow approach in describing what would qualify for this exception. While we appreciate the agency pushing the industry not to leverage costs to restrict the flow of information, the application of this exception will be challenging for ONC. Again, we urge significant provider education and the promotion of a toll-free number and email/website complaint process.

ONC Proposal (Page 7542)

We propose to establish an exception to the information blocking provision that would permit an actor to decline to provide access, exchange, or use of EHI in a manner that is infeasible, provided certain conditions are met.

MGMA Response

We support including an exception that would permit a practice to decline to provide access, exchange, or use of EHI in a manner that is infeasible. With so many proposed considerations in the rule, however, we highly recommend that ONC issue guidance to assist practices understand when this exception would apply and what steps practices would be required to take to apply it. For example, the Proposed Rule stipulates that a practice "must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information." "Timely manner" is one of the terms that needs clarification. We would urge ONC to permit sufficient time for practices to work with patients to meet their needs, and not less than 30 days.

ONC Proposal (Page 7544)

We propose to establish an exception to the information blocking provision that would permit actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms, provided that certain conditions are met.

MGMA Response

We support establishing an exception to the information blocking provision that would permit actors to license interoperability elements on reasonable and non-discriminatory terms. With so many proposed considerations in the rule, however, we highly recommend that ONC issue guidance to assist practices understand when this exception would apply and what steps practices would be required to take to apply it.

ONC Proposal (Page 7550)

We propose to establish an exception to the information blocking provision for certain practices that are reasonable and necessary to maintain and improve the overall performance of health IT, provided certain conditions are met.

MGMA Response

We support establishing an exception to the information blocking provision for certain practices that is reasonable and necessary to maintain and improve the overall performance of health IT. With so many proposed considerations in the rule, however, we highly recommend that ONC issue guidance to assist practices understand when this exception would apply and what steps practices would be required to take to apply it.

ONC Proposal (Page 7524)

The exception may permit certain restrictions on the disclosure of an individual's EHI in circumstances where a licensed health care professional has determined, in the exercise of professional judgement, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person.

MGMA Response

We support establishing an exception that permits certain restrictions on the disclosure of an individual's EHI in circumstances where a licensed health care professional has determined, in the exercise of professional judgement, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person. With so many proposed considerations in the rule, however, we highly recommend that ONC issue guidance to assist practices understand when this exception would apply and what steps practices would be required to take to apply it.

ONC Proposal (Page 7527)

For example, we believe that, unless required by law, actors should not be compelled to share EHI against patients' wishes or without adequate safeguards out of a concern that restricting the access, exchange, or use of the EHI would constitute information blocking. This could seriously undermine patients' trust and confidence in the privacy of their EHI and diminish the willingness of patients, providers, and other entities to provide or maintain health information electronically in the first place.

MGMA Response

This is an important section of the information blocking regulatory preamble. While we are supportive of patient information moving from a practice to an authorized entity for purposes of treatment, payment, or healthcare operations (TPO), we also contend that patients must have the right to restrict the movement of that data. Many medical specialties deal with extremely sensitive patient data and all collect PHI. They should have the right to have a conversation with their patients regarding the appropriate dissemination of sensitive health information. We oppose any effort to restrict the physician-patient relationship.

ONC Proposal (Page 7532)

We propose that in. This condition would provide basic assurance that the purported privacy practice is directly related to a specific privacy risk and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.

MGMA Response

We agree that in order for a practice to qualify for this exception, the policy must be implemented in a consistent and nondiscriminatory manner. This exception is potentially an important one for practices as many may have already established policies to protect the confidentiality of their patients' data and not for the purposes of interfering with the access or exchange of health information.

Attestation and Developer Noncompliance

ONC Proposal (Page 7501)

We propose that, as a Maintenance of Certification requirement for the ''attestations'' Condition of Certification, health IT developers must submit their attestations every 6 months (i.e., semiannually). We believe this would provide an appropriate ''attestation period'' to base any enforcement actions, such as by ONC under the Program or by the Office of the Inspector General under its Cures Act authority. We also believe this 6-month attestation period properly balances the need to support appropriate enforcement actions with the attestation burden placed on developers. We will determine when the first attestation will be due depending on when the final rule is published. We require attestations to be due twice a year, likely in the middle and end of the calendar year.

MGMA Response

Leveraging an attestation approach alone may not allow for an appropriately detailed review of the software. Numerous systems must be evaluated, and this complex process would be more appropriately evaluated by subject matter experts. The use of non-biased objective third-party certification/accreditation to assure the compliance with basic systems and compliance security, cybersecurity, operations and compliant communications could prove an ideal methodology to assure stakeholder-trust is spread throughout the participants of the HIN.

ONC Proposal (Page 7505)

We propose that if ONC determines that a health IT developer is noncompliant with a Condition of Certification (i.e., a non-conformity), ONC would work with the health IT developer to establish a corrective action plan (CAP) to remedy the issue through the processes specified in § 170.580(b)(2)(ii)(A)(4) and (c). We note that a health IT developer may be in noncompliance with more than one Condition of Certification. In such cases, ONC will follow the proposed compliance enforcement process for each Condition of Certification accordingly, but may also require the health IT developer to address all violations in one CAP for efficiency of process.

MGMA Response

Noncompliance on the part of an EHR developer with a specific condition of certification is a significant issue for physician practices. Practices rely on these vendors to meet ONC and CMS requirements. Should the vendor not appropriately support these requirements, the practice could be at risk for significant penalties as part of the QPP or ONC enforcement actions related to information blocking.

Practices also struggle when an EHR product has been decertified by ONC. Decertification of their EHR could result in a physician practice being unable to successfully participate in the QPP. Even if the eligible clinicians or group practice received a hardship exception from the MIPS

Promoting Interoperability requirements, failed software could result in the clinicians or group being unable to successfully participate in the other components of the QPP.

ONC Proposal (Page 7504)

We propose in § 170.581 that if a health IT developer under ONC direct review for non-compliance with a Condition of Certification failed to work with ONC or was otherwise noncompliant with the requirements of the CAP and/or CAP process, ONC could issue a certification ban for the health IT developer (and its subsidiaries and successors). A certification ban, as it currently does for other matters under § 170.581, would prohibit prospective certification activity by the health IT developer.

MGMA Response

We support the proposal that when a health IT developer under ONC direct review for non-compliance with a Condition of Certification failed to work with ONC or was otherwise noncompliant with the requirements of the CAP and/or CAP process, ONC would issue a certification ban for the health IT developer (and its subsidiaries and successors). We cannot have bad actors continuing to produce products that fail to meet ONC requirements. However, we recommend that ONC work closely with CMS to ensure that practices that have previously implemented these products are not unfairly penalized in their participation in any of the CMS reporting programs.

ONC Proposal (Page 7524)

When a clinician or other health IT user may know or reasonably suspect that specific EHI in a patient's record is or may be misattributed, either within a local record or as received through EHI exchange, it would be reasonable for them to avoid sharing or incorporating the EHI that they know would, or reasonably suspect could, propagate errors in the patient's records and thus pose the attendant risks to the patient…A health IT developer of certified health IT could not, for example, refuse to provide a batch export on the basis that the exported records may contain a misidentified record. Similarly, a health care provider that identified that a particular piece of information had been misattributed to a patient would not be excused from exchanging or providing access to all other EHI about the patient that had not been misattributed.

MGMA Response

The issue of accurately identifying the patient when sharing medical records is critical. ONC appropriately recognizes the importance from both a patient safety and interoperability standpoint of being able to connect the right patient with their records. However, we are concerned that ONC indicates in the Proposed Rule that a health IT developer cannot refuse to provide a batch export on the basis that the exported records may contain a misidentified record. Similarly, a practice that flagged misattributed patient information would not be excused from exchanging or providing access to all other EHI about the patient that had been misattributed.

We assert that this is the wrong approach. The agency seems to suggest that transmitting inaccurate health information is better for the delivery of care than transmitting no information. We disagree. Physicians making clinical decisions based on inaccurate data is clearly a patient safety issue and can result in harm to the patient. Physicians should be permitted to use their professional judgement in determining if the information to share is inaccurate. It should not be considered data blocking if the physician withholds information that they believe was not an appropriate part of the patient's record.

ONC Proposal (Page 7533)

We believe that it would be reasonable that non- covered actors would, at minimum, post their privacy notices, or otherwise describe their privacy-protective practices, on their websites.

MGMA Response

We concur with ONC that it would be reasonable that non-covered actors would, at minimum, post their privacy notices, or otherwise describe their privacy-protective practices, on their websites.

Requests for Information

ONC Proposal: Pricing RFI (Page 7513)

ONC has a unique role in setting the stage for such future actions by establishing the framework to prevent the blocking of price information. Given that price information impacts the ability of patients to shop for and make decisions about their care, we seek comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking. In addition, the overall Department seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

MGMA Response

In general, MGMA supports the call for price transparency. However, simply requiring physicians and other providers to disclose their walk-in charges for common procedures is not the solution. Patients are increasingly responsible for co-insurance payments based on a percentage of the charges allowed under their insurance plans, so it is essential that they know the amount their insurance will pay for services received.

Most physicians participate in 20 or more insurance plans, and because many insurers have varying reimbursement rates for different products, it is not unusual for a service to have as many as 100 prices in a physician practice. Accordingly, the physician is unlikely to be able to produce the price that will be paid by a particular insurer, for a particular patient's plan, for a particular procedure. Furthermore, contractual restrictions in health plan contracts often prohibit medical practices from releasing pricing information. These restrictions often fall under confidentiality provisions that classify health plans' pricing structures as proprietary information. As a result, medical practices cannot disclose this information, even to patients.

"Future payment" is included by ONC in the definition of EHI. While it is laudable to seek to provide patients with the future cost of a medical service, it is simply not feasible in most instances. Further, in the vast majority of cases, patients are far less interested in ascertaining the cost of the service than they are in their specific out-of-pocket expenses. Should a patient present at a practice covered, for example, under a commercial health plan product, it would be extremely difficult and administratively burdensome for a practice to determine ahead of time what the cost of the service would be and what the patient out-of-pocket expense would be.

Several transactions need to occur prior to the practice receiving the full information from the commercial health plan rated to the cost of a service. For example, the practice will verify first if the patient's health insurance coverage is valid and whether the benefits package includes the service in question. Next, the practice may need to begin a prior authorization process with the health plan, a process that can take hours, days, or even weeks to complete. Once that process is finalized, and the practice has an estimate of what the costs will be, there is no guarantee that

after the service is performed and the claim is submitted by the practice to the health plan, that the expected cost for the service, or the patient's out-of-pocket expenses, will be the same as the estimate.

For insured patients, health plans should serve as the principal source of price information for their members. Health plans should innovate with different frameworks for communicating price information to insured patients.

Transparency tools for insured patients should include some essential elements of price information, including:

- The total estimated price of the service;
- A clear indication of whether a specific provider is in the health plan's network and information on where the patient can try to locate a network provider;
- A clear statement of the patient's estimated out-of-pocket payment responsibility; and
- Other relevant information related to the provider or the specific service sought (i.e. clinical outcomes, patient safety, patient satisfaction scores)

Insured patients should be alerted to the need to seek price information from out-of-network providers. To ensure valid comparisons of provider price information, health plans and other suppliers of such information should make transparent the specific services that are included in the price estimate.

The provider should be the principal source of price information for uninsured patients and patients who are seeking care from the provider on an out-of-network basis.

Price transparency frameworks for uninsured and out-of-network patients should reflect the following basic considerations:

- Providers should offer an estimated price for a standard procedure without complications and make clear to the patient how complications or other unforeseen circumstances may increase the price.

- Providers should clearly communicate preservice estimates of prices to uninsured patients and patients seeking care on an out-of-network basis.

- Providers should clearly communicate to patients what services are—and are not—included in a price estimate. If any services that would have significant price implications for the patient are not included in the price estimate, the provider should try to provide information on where the patient could obtain this information.

- Providers should give patients other relevant information (i.e. clinical outcomes, patient safety, patient satisfaction scores) where available.

There is a movement in the industry to develop a real-time benefit tool (RTBT). There are currently several RTBT products available in the pharmacy environment, with each providing real-time out-of-pocket expenses at the point of care as well as therapeutic alternatives for all patients. These products permit the clinician to have a discussion with the patient regarding cost and medication alternatives and can be an effective tool in the care delivery process.

However, although development of a standard is underway by the National Council of Prescription Drug Programs, there is currently no national RTBT standard, and none of the available products capture and present information from all health plans. On the medical services side, there are no RTBT products available to assist clinicians and patients understand costs in real-time.

Providing cost information, especially in real-time when it will be most valuable to the patient, would be extremely difficult, if not impossible. However, RTBT holds the promise of providing patients with helpful pricing information, but even more importantly, critical clinical information to both the patient and physician.

Recommendations for achieving price transparency:

- Require health plans to release fee schedules showing total allowed charges and methods used to calculate fees to physicians and hospitals as part of their provider contracting process. Practices are unable to provide accurate price information to patients if insurers are not required to provide fee schedule information to them.

- Require that health plan contracts with physicians and hospitals clearly specify that disclosure of insurer fee-schedule information to patients, for services that are to be provided to the patient by the physician or hospital and charged to that insurer, is permissible. ONC should conduct research to investigate elements of fee information most valuable to patients and consumers, especially those in preferred provider organizations, health savings accounts and high-deductible health plans, and for self-pay patients.

  Similarly, ONC should investigate whether health plan use of efficiency ratings of medical practices or individual physicians is useful to consumers in estimating their out-of-pocket costs for certain conditions. If not, additional research should be undertaken to investigate what is most beneficial for consumers.

- Focus on providing effective tools that allow practices to make information on walk-in fees available to patients on request, along with any policies regarding discounts offered for prompt payment. Further, encourage but do not require practices to make allowable charges for specific procedures, for a particular insurer and plan, available to patients covered by that insurer and plan upon request (as permitted by insurer contracts).

- Overall, we urge ONC to focus less on adding new administrative burdens on practices and focus more on working with CMS and the private sector to release a standardized RTBT for pharmacy and develop an RTBT standard for medical services.

ONC Request for Information: Patient Matching RFI (Page 7555)

In this Request for Information (RFI), we seek comment on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching.

MGMA Response

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

Patient identification is an acute problem as the nation continues to invest in EHR technology with the patient's electronic "address" often differing across EHR systems. There are significant

benefits to adoption of flexible commercial market solutions that consistently demonstrate high degrees of accuracy now and in the future. Identifying the patient correctly is essential for healthcare providers, insurance providers, and others exchanging data for both clinical and administrative purposes. Most importantly, patient care is improved, and patient safety is enhanced when health information is accurately transmitted between healthcare entities, especially in emergency situations.

While numerous patient-matching and identity management initiatives have been undertaken, there currently is no common patient matching strategy that has been adopted by the healthcare industry. Governmental and commercial market collaboration can foster the adoption of such technology solutions and allow them to improve and adapt as technology advances and new techniques are identified. As well, if these solutions are to be effective, they must be easily-implementable and broadly adopted by the industry.

Through the implementation of these recommendations, patient identification accuracy can be greatly increased as new technologies open up access for consumers to increase their literacy regarding health information technology as a means of managing their own health information. It is expected that by strengthening patient identification processes, improvements can be made in linking patients to correct medical records and in information flow at lower costs with reduced medical errors and medical test redundancy. Additionally, it is expected that these efforts would directly correlate to a reduction in fraud and abuse.

Ineffective patient matching can have patient safety and cost ramifications. Patients may receive inappropriate care and face the possibility of medical errors if information used for treatment is missing or inaccurate; one in five hospital chief information officers surveyed said that patient harm occurred within the last year due to a mismatch.

To accurately match records held at different health care facilities, organizations typically compare patients' names, dates of birth, and other demographic data to determine if records refer to the same individual. Health care facilities use algorithms to conduct these matches, and also employ staff to manually review records. This process often fails to accurately link records because of typos entered into the system; similarities in names, birth dates or addresses among different patients; changing information, such as when individuals move or get married; and many other reasons.

While some private sector technologies—such as referential matching, wherein third-party data are used to support matches—show promise, market forces have been unable to solve the patient matching problem for decades. In fact, patient matching requires collaboration between unaffiliated organizations, even competitors, that lack incentive to agree to a set of standards or develop systems that seamlessly exchange information.

ONC's recent regulations already propose embedding address in the USCDI, but the agency could further improve match rates by requiring use of the USPS standard. To further promote the use of this standard, ONC should also coordinate with USPS to ensure that health care organizations can use the postal service's online, API-based tool—or another easily accessible mechanism—to convert addresses to the USPS standard. There may also be scenarios—such as for military personnel stationed abroad—where the use of the USPS standard is not feasible. ONC could restrict use of the USPS standard to domestic, non-military addresses if challenges arise in the broader use of the standard.

Specific responses to ONC and CMS questions in the patient matching RFI

ONC seeks input on various approaches to address patient matching, minimum data requirements, and measures to assess performance of different solutions.

- *ONC requests input on the potential effect that data collection standards may have on the quality of health data that is captured and stored. ONC also requests input on solutions that may increase the likelihood of accurate data capture, including the implementation of technology that supports the verification and authentication of certain demographic data*. As mentioned above, use of the USPS standard for address would improve match rates and does not require the capture of information in this format given the availability of online tools to conduct the conversion.

- *ONC solicits information on additional attributes that could aid patient matching, and new data that could be added to the USCDI or further constrained within it to support patient matching*. ONC should examine additional data routinely collected in EHRs to also use for matching—such as email address, health insurance ID, mother's maiden name, and others.

- *ONC requests input on the potential effect that data collection standards may have on the quality of health data that is captured and stored and possible impact on accurate patient matching. ONC also requests input on solutions that may increase the likelihood of accurate data capture, including the implementation of technology that supports the verification and authentication of certain demographic data.*

  Better standards for address (according to the U.S. Postal Service standard) would improve match rates. Standardizing according to USPS does not require the capture of the data in this standard, but rather its transformation into this standard once captured (e.g. via an API). Software that automatically converts addresses to the USPS standard is common in commercial internet transactions and could be leveraged in health care. ONC should work with USPS to make its address verification APIs widely available for health care.

- *ONC requests input on additional attributes that could aid patient matching, minimum set of elements for collection and exchange, and data that could be added to the USCDI. ONC also requests information on new data that could be added to the USCDI or further constrained within it to support patient matching*. In addition to specifying use of the USPS standard for address, ONC should examine additional data routinely collected in EHRs to use for matching—like email address, health insurance ID, mother's maiden name, and others. ONC should add those data elements that are already collected to the USCDI.

- *ONC also seeks comments on potential solutions that involve patients in the capture, update and maintenance of their own demographic and health data.* Patients could validate their demographic information by verifying their mobile phone number and other data. In addition, EHRs could support smartphone applications that use standard APIs to allow patients to update their demographic data. ONC and industry partners could pilot these approaches.

- *ONC requests input on other innovative approaches to address patient matching*. The agency should explore promising new approaches to patient matching that have not yet been widely used in healthcare including biometrics approaches such as fingerprint or facial recognition scans.

- *ONC seeks input on performance measures and indicators that can be used to evaluate patient matching algorithms*. Benchmarking different approaches would help shed a

spotlight on matching deficiencies and the wide variation in quality across different algorithms. Technology developers could then use that information to improve their algorithms, and health care providers could adopt the most promising approaches. ONC should work with CMS to determine how to benchmark different matching approaches; this likely requires the identification of a large, real-world data set to test different algorithms.

The use of real-world data, rather than synthetic data, is essential given that some innovative approaches—such as referential matching—use third-party databases to support their algorithms. ONC or CMS may be able to indentify grantmaking authorities or other policies to obtain such a data set for benchmarking. This benchmarking could assess duplicate creation rates, the number of records correctly matched, and the frequency with which records are incorrectly merged.

- *CMS requests information on whether to require program participants use a patient matching algorithm or solution with a "proven" success validated by HHS or a third party*. CMS should examine how to benchmark different approaches to patient matching to provide better information on the variation across matching algorithms and to highlight current limitations. However, benchmarking—on its own—will not improve match rates; CMS should work with ONC to optimize the use of demographic data (including adoption of the USPS standard for address and the use of additional data elements).

- *CMS requests information on whether to expand recent Medicare ID card efforts by requiring a CMS-wide identifier for all beneficiaries and enrollees in healthcare programs under its administration and authority*. Implementing an agency-wide identifier may help CMS better serve beneficiaries and improve matching. However, this approach is still insufficient to address matching on a nationwide scale.

  We note that a unique identifier would still face limitations in matching patients to information prior to enrollment in federal health insurance programs, and they are still susceptible to errors (e.g. typos that exist today with the use Social Security Numbers). Given those limitations, even if CMS pursues broader use of a CMS-wide identifier, the agency should still push forward with optimizing the use of demographic data (including adoption of the U.S. Postal Service standard for address and the use of additional data elements).

- *Finally, CMS requests information on whether it should advance more standardized data elements across all appropriate programs for matching purposes, perhaps leveraging the USCDI proposed by ONC*. CMS should work with ONC to advance both the use of the USPS standard for address and the addition of other elements—like email address—to the USCDI.

Patient matching recommendations:

- <u>Initiate public-private sector collaboration</u>.

  - Identify best practices related to private-sector patient matching solutions and make recommendations to the HHS Secretary. This effort should include exploring expanding the USCDI to include additional criteria such as email address that could be leveraged for patient matching purposes. Recommendations should ensure sufficient flexibility to account for potential new technologies and solutions.

  - Develop pilots of one or more of these identified best practices.

- Explore having HHS set a floor for error matching rates. Once they have met the "floor," permit entities the flexibility to determine what solution works best for them.

- Explore having ONC provide certification and/or oversite over patient matching solutions.

- Explore enforcement (i.e. data blocking) safe harbors for entities making good faith efforts at patient matching and meeting appropriate patient matching guidelines.

- Identify potential patient matching solution dissemination strategies and make recommendations to the HHS Secretary.

- Support the standardization of some demographic data, particularly applying the USPS standard to an individual's address.

  - ONC has taken the first step to include address among the demographic data elements proposed in the USCDI. ONC should build on the addition of address to the USCDI by specifying the use of the USPS standard for address. ONC should incorporate this change in the final rule.

  - ONC should explore publicly available options for APIs that can transform address into the USPS standard. Commercial options exist for this transformation, and the USPS has an API that enables this transformation. ONC should work with the USPS to ensure that this API is available for health record matching.

- Adopt additional data elements for patient matching.

  - ONC should advance the use of regularly collected demographic data elements for patient matching. ONC currently requires EHRs to make some demographic data—such as name, birth date, and sex—available, and proposes to add address and phone number to the USCDI. However, health records contain other demographic data routinely collected that aren't typically used or made available to match records. For example, email addresses are typically already being captured by practices. The documentation of email is likely higher today, given the adoption of patient-facing tools, like portals, that often require emails to register.

  - ONC could improve match rates by identifying and including in the USCDI readily available data elements—such as email address, mother's maiden name, or insurance policy identification number—that health information technologies should use for matching.

- Finally, in concert with the healthcare industry, CMS and ONC should initiate an awareness and education campaign aimed at critical healthcare stakeholders, with emphasis on patients, practices, and HIEs.

There are a number of issues that should be considered as a national patient matching strategy is developed. These include the potential employment of mobile technology and the use of alternative matching criteria such as email addresses, health insurance ID, mother's maiden name, and others. Further, CMS and ONC should examine how to benchmark different approaches to patient matching to provide better information on the variation across matching algorithms and to highlight current limitations.

Conclusion

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

With the publication of this Proposed Rule, ONC has taken on the formidable task of reshaping public policy in an effort to create a healthcare environment that leads to improved patient care and more efficient delivery of care. We look forward to continuing to work with ONC and other federal agencies to facilitate the physician practice transition to effective and efficient health IT and ensure that the promise of improving the nation's healthcare system through technology becomes a reality. Should you have any questions regarding these comments, please contact Robert Tennant, Director, Health Information Technology Policy, at 202.293.3450 or rtennant@mgma.org.

Sincerely,

/s/

Anders Gilberg, MGA
Senior Vice President, Government Affairs