



**Association of
American Medical Colleges**
655 K Street, NW, Suite 100, Washington, DC 20001-2399
T 202 828 0400
aamc.org

Via Electronic Submission (www.regulations.gov)

June 3, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
Mary E. Switzer Building
330 C Street SW
Washington, DC 20201

RE: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule [RIN 0955-AA01]

Dear Dr. Rucker:

The Association of American Medical Colleges (AAMC) appreciates the opportunity to comment on the proposed rule “21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program,” 84 *Fed. Reg.* 7424 issued by the Office of the National Coordinator for Health Information Technology (ONC).

The AAMC is a not-for-profit association dedicated to transforming health care through innovative medical education, cutting-edge patient care, and groundbreaking medical research. Its members are all 154 accredited U.S. and 17 accredited Canadian medical schools; nearly 400 major teaching hospitals and health systems, including 51 Department of Veterans Affairs medical centers; and more than 80 academic societies. Through these institutions and organizations, the AAMC serves the leaders of America’s medical schools and teaching hospitals and their more than 173,000 full-time faculty members, 89,000 medical students, 129,000 resident physicians, and more than 60,000 graduate students and postdoctoral researchers in the biomedical sciences. Together, these institutions and individuals are the American academic medicine community.

The AAMC applauds ONC for its efforts to advance interoperability, support the access, exchange, and use of electronic health information, and prevent information blocking. We share ONC’s commitment to ensuring that patients and clinicians have the increased ability to access electronic health information to make informed health decisions through secure and seamless exchange of electronic health information. The focus of efforts to improve interoperability should be on what is needed for high quality clinical management of patients receiving care from providers as they move through the health care system. At the same time, it is critical to also protect the privacy and security of patient health information.

Many of the AAMC's member institutions were early adopters of electronic health record (EHR) technology; they have helped to pioneer its development and use and are committed to providing quality care using these systems. While we support ONC's efforts, the AAMC would like to highlight provisions in the proposed rule that we support, aspects that could be strengthened, and areas of concern that could increase burden, health care costs, and potentially jeopardize privacy and security (confidentiality of information). These include:

Updates to the 2015 Edition Certification Criteria:

- ***Electronic Health Information (EHI) Export:*** ONC should finalize the requirement that HIT systems be able to export electronic health data to allow patient access and smoother transitions between systems.
- ***Data Segmentation for Privacy:*** ONC should seek further stakeholder input concerning options for improving data segmentation for privacy and consent management before requiring this feature in certified technology. Existing technology does not enable providers to tag portions of data as sensitive to ensure that the privacy of this data is not jeopardized, and stakeholders must agree on best practices.
- ***Implementation Time Frames:*** ONC must provide sufficient time for vendors to comply with the new certification criteria and for providers to deploy the updates to the systems. ONC and CMS should coordinate to allow, at the very least additional implementation time beyond the 24 months proposed in the rule.

Conditions and Maintenance of Certification:

- ***Prohibition on Restricting Communications:*** ONC should finalize the requirement that the HIT developer not prohibit or restrict communications regarding the usability of its HIT, the interoperability of its HIT, the security of its HIT, users' experiences of its HIT, business practices of its HIT related to exchanging EHI, and the manner in which a user of its HIT has used such technology.
- ***Trusted Exchange Framework and Common Agreement (TECFA):*** ONC should require certain HIT developers to participate in TECFA as an assurance that the developer is not acting as an information blocker or inhibiting the appropriate exchange, access, and use of EHI.

Application Programming Interfaces (APIs)

- ***Standardizing APIs:*** ONC should set forth requirements related to standardization and transparency associated with APIs, while also ensuring protections are in place to promote the privacy and security of EHI.
- ***Adoption of Fast Healthcare Interoperability Resources (FHIR) Standard:*** ONC should adopt its proposed regulatory approach that allows the time necessary for the industry to adopt and implement Release 4, while maintaining certification under Release 2 in the interim.
- ***Authenticity Verification:*** The AAMC supports the proposal to permit an authenticity verification but urges ONC to consider a longer timeframe to complete the verification process and additional vetting of application developers.

- **Informing Patients:** EHR API vendors that are certified by ONC should also certify that the applications their APIs connect to meet established best practices and privacy guidelines and provide a model notice to patients regarding how their information might be used by the app.
- **Permitted Fees:** ONC should reconsider its proposals related to permitted fees, as they are likely to place significant financial burden on the API Data Providers. ONC should consider balancing the costs associated for API development and deployment across both API Data Providers and certain API Users, to ensure that third-party software application developers are contributing.

Information Blocking

- **Innocuous and Beneficial Activities Should Not be Considered Information Blocking:** The AAMC supports efforts to deter practices that unnecessarily impede the flow of EHI or its use to improve health and the delivery of care. We believe it is important that activities that are innocuous and beneficial are not considered violations of the information blocking provision.
- **Clear, Predictable, and Feasible to Implement:** To minimize burden for providers, the information blocking provisions and exceptions need to be clear, predictable, and feasible to implement, and sensitive to practical challenges that may prevent access, exchange, or use of EHI.
- **Realistic Time Frames for Compliance:** ONC must provide sufficient time for “actors” to comply with the information blocking provisions after the rule is finalized. At a minimum, we recommend no enforcement of the information blocking provisions for a period of at least 24 months after the effective date of the rule.
- **Definition of Electronic Health Information (EHI):** The proposed E H I definition that would apply to information blocking is overly expansive and should be revised to include only the USCDI data elements stored within the EHR. Payment information should not be included in the definition of EHI. Non-observational information should not be included within the definition of EHI as such information is not necessary for direct patient care and its inclusion could potentially deter reporting of adverse events and quality improvement initiatives.
- **Definition of Health Information Network and Health Information Exchange:** Providers should not be included in the definitions of Health Information Network or Health Information Exchange.
- **Information Blocking Exceptions:** ONC should provide more examples and guidance on the exceptions and the type of documentation that would be acceptable to support the criteria.
- **Exception: Promoting the Privacy of EHI:** Information blocking rules must be aligned with HIPAA privacy and state privacy laws to the extent possible. Providers should not be compelled to share EHI against a patient’s wishes or without adequate safeguards. It should be recognized that in some circumstances obtaining patient consent can be outside the direct control of the provider.
- **Exception: Promoting the Security of EHI:** ONC should clarify that this exception allows providers to be proactive when promoting the security of EHI rather than taking a reactive stance.
- **Disincentives for Health Care Providers:** There is no need to establish new disincentives to information blocking for providers since the Promoting Interoperability Programs for hospitals and eligible clinicians have penalties that should deter information blocking.

Patient Matching Request for Information

- ***Collaboration on Patient Matching Solutions:*** Providers, software developers and other healthcare organizations should collaborate on the identification of a common set of data elements based on federal adopted standards to support patient matching. HHS should participate and provide technical assistance to the private sector in developing standards for patient matching.

UPDATES TO THE 2015 EDITION CERTIFICATION CRITERIA

Implementation Timelines

ONC is proposing a significant set of changes to EHR certification requirements, which will address many concerns regarding interoperability. However, the proposed timeline of 24 months for providers and developers to create, test, certify, purchase, upgrade, implement and use brand new technology is infeasible. Typically, vendors need 18-24 months for development and providers need at least 12 months to deploy major updates to their EHR systems. The proposed concurrent timelines may not provide sufficient time to safely and effectively implement new EHR technology. ONC and CMS should coordinate to allow, at the very least, additional implementation time beyond the 24 months proposed in the rule.

Electronic Health Information (EHI) Export

ONC proposes to add a new certification criterion of “EHI export” to the 2015 Edition and to the 2015 Edition Base EHR definition, along with proposing the corresponding removal of the existing data export criterion at 42 CFR § 170.315(b)(6). This new “EHI export” criterion is intended to act as a step towards providing continuous access to patients’ EHI through open, standards-based APIs, but ONC is clear that the minimum requirement is for a discrete data export capability, and not persistent, real-time EHI access. HIT developers would need to implement the capability to electronically export EHI produced and managed in a health IT system in a computable format within 24 months of the final rule’s effective date. HIT developers must make publicly available documentation for the interpretation and use of EHI. ONC notes that this proposed criterion intentionally refers to EHI rather than EHRs, and thus covers EHI stored outside of EHRs (e.g., imaging information stored electronically, but not within the EHR). In terms of scope of the requirement, ONC requests feedback on whether it should require the EHI export capability to permit time-delimited requests (e.g., “the past month of EHI”). Additionally, ONC proposes that the EHI exports should include all EHI that the HIT system produces and electronically manages for a patient or a group of patients.

The EHI export function is intended for both patient access (a single patient’s data upon a valid request from the patient or a user on the patient’s behalf) and system transition access (all patients’ EHI when a provider seeks to change HIT systems). Regarding the patient access use, ONC envisions the typical user will be a provider’s office staff requesting the EHI export on behalf of a patient. In order to mitigate privacy concerns with single patient requests, ONC proposes to allow limits on the ability of users who can create EHI export files, at the discretion of the provider organization implementing the technology, to either a specific set of identified users or as a system

administrative function. ONC specifically requests feedback on whether access should be further limited to only allow the patient or his/her authorized representative to be the requestor of the patient's EHI.

The AAMC supports the requirement that HIT systems be able to export electronic health data, especially in the case of a provider seeking to transition to a new EHR system. We agree that this will enable smoother transitions between systems. In response to the consideration of time-delimited requests, we would ask ONC to consider current capability and whether to require all requests to be time-delimited (i.e., always requiring the request to include a span of time) rather than requests without a timeframe.

The proposed scope of EHI included for export is concerning, and **the AAMC believes the EHI export should be limited to the U.S. Core Data for Interoperability (USCDI) data elements within the EHR**, which we recommend as a revised definition of EHI. In addition, for EHI export purposes, ONC should consider requiring the capability to export images; for example, imaging is not included in the USCDI standards at this time. The scope of the EHI is also important when considering the server bandwidth for providers to process EHI export requests (both the size of the EHI data and the volume of requests to be processed). We appreciate that ONC is not requiring that EHI exports occur instantaneously (or in "real time") and that the proposed requirement is a step towards persistent access to a patient's EHI. Timely access to data is critical for patient care, but HIT system servers must have the bandwidth to process exports in addition to processing the regular data access required in the normal course of care delivery. **Until such time that EHI exports can be processed without impacting server capacity for the delivery of care, EHI exports should be allowed to be processed during off-peak hours as a timely response to discrete export requests.**

Regarding potential limitations on who should be allowed to request a single patient's data, the AAMC believes the proposal strikes a balance that allows for appropriate limits regarding EHI exports and ensures privacy and security of the data. Providers should be allowed to limit to a patient or patient's representative request in certain circumstances. Providers should allow for another provider's request for a patient's export if it is directly authorized by the patient. **The AAMC supports ONC's proposal to allow two types of limits on the ability of users to create EHI export files, at the discretion of the provider.**

We recommend that ONC provide additional guidance and clarification about the costs associated with proposed EHI export. Currently under some state laws and federal law there are limits to what a provider can charge a patient for a copy of his or her data. These fees are nominal and are intended to balance patient access with the costs associated with such access, primarily the time and materials to vet such requests to ensure they are valid, and that data is shared appropriately and in compliance with state and federal law. The AAMC believes it is reasonable for providers to recover some costs associated with providing access, similar to what is currently allowed under HIPAA.

Data Segmentation for Privacy and Consent Management Criteria

ONC proposes to remove the existing Data Segmentation for Privacy (DS4P) criteria (DS4P-send and DS4P-receive) and replace with new DS4P criterion using supported by either Consolidated-Clinical Document Architecture (C-CDA) or FHIR-based exchange standards. These new C-CDA

criteria for DS4P-send and DS4P-receive would require capability for security tagging at the document, section, and entry levels.

ONC has also worked with the Substance Abuse and Mental Health Services Administration (SAMHSA) to develop a Consent2Share application designed to integrate with existing FHIR systems for data segmentation and consent management. SAMSHA created a FHIR implementation guide, Consent IG, to describe how Consent2Share uses the FHIR Content resource to represent patient consent for treatment, research, or disclosure. ONC proposes to add an additional new criterion “consent management for Apps” for support of data segmentation and consent management in accordance with the FHIR-based Consent IG. Certification to this criterion would be discretionary for HIT developers.

The AAMC supports efforts to enhance capability for security tagging but urges ONC to take more time to consider options for implementation. Current EHR technologies do not have the capability to tag individual data elements as private within a patient’s record. Before enforcing this requirement, HIT developers and vendors need additional time to build-out full data segmentation capabilities, and also time to implement and test the enhanced technology in the clinical setting. Additionally, it’s unclear whether ONC envisions DS4P to cover all data in the medical record, including provider notes. If the vision is expansion, there should be a transition period to allow providers to segment the notes that are appropriate to share for treatment purposes from other notes.

Additionally, while consent management at a granular level has the potential to ease patient consent documentation burden, there is concern that it could prevent the sharing of medical information that is critical to patient care. **ONC should gather further stakeholder input on options for improving privacy and consent management data segmentation before finalizing as criteria for certification.** Ideally in the future there will be a system that allows data to flow between treatment providers while allowing tagging to ensure sensitive data is adequately protected.

CONDITIONS AND MAINTENANCE OF CERTIFICATION

Assurances

The Cures Act requires that as a Condition of Maintenance of Certification under the Program, a HIT developer provide assurances to the Secretary that it will not take any action that constitutes information blocking. ONC proposes to establish more specific Conditions and Maintenance of Certification for a HIT developer to provide assurances that it does not take any action that may inhibit the appropriate exchange, access, and use of EHI.

Trusted Exchange Framework and the Common Agreement (TECFA) – Request for Information

ONC seeks feedback as to whether certain HIT developers should be required to participate in TECFA as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. Such a requirement would need to be proposed in subsequent rulemaking, and would apply to HIT developers that provide services for connection to health

information networks (HIN), including routing EHI through a HIN or responding to requests for EHI from a HIN.

The AAMC supports requiring certain HIT developers to participate in TECFA as an assurance that the developer is not acting as an information blocker or inhibiting the appropriate exchange, access, and use of EHI. **We suggest that ONC establish criteria for the types of HIT developers that would be required to participate in TECFA.**

Communications

The Cures Act requires that HIT developers do not prohibit or restrict communication regarding the usability of HIT, the interoperability and security of HIT, relevant information regarding HIT users' experience with the HIT, business practices of developers related to exchanging EHI, and the manner in which a HIT user has used such technology. ONC proposes to implement this Condition of Certification as a broad prohibition against HIT developers imposing prohibitions and restrictions on protected communications, allowing developers to impose prohibitions on protected communications only in certain narrowly defined circumstances.

Condition of Certification Requirements

ONC specifically proposes to require that a HIT developer does not prohibit or restrict communications regarding: the usability of its HIT, the interoperability of its HIT, the security of its HIT, users' experiences of its HIT, business practices of its HIT related to exchanging EHI, and the manner in which a user of its HIT has used such technology. Additionally, ONC proposes unqualified protection (meaning a HIT developer could not prohibit or restrict communication of any information or materials whatsoever) for the following specific communications: making a disclosure by law; communicating information about adverse events, hazards, or other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations; and communicating information about cybersecurity threats and incidents to government agencies; communicating information about information blocking or other unlawful practices to government agencies; or communicating information about a HIT developer's failure to comply with a condition of certification or another requirement to ONC or an ONC-Authorized Certification Body (ONC-ACB).

ONC proposes that HIT developers be permitted to prohibit and restrict communications of their employees or contractors, and communications that disclose information about non-user-facing aspects of the developers. Additionally, a HIT developer could prohibit or restrict communications that would infringe on its intellectual property rights, provided the developer did not prohibit or restrict communications that would be a fair use of copyright work and the developer did not prohibit the communication of screenshots of its HIT (subject to the enumerated limits).

The AAMC supports the goal of improving transparency about the functionality of HIT in the field. Past industry practices have limited knowledge sharing about the functionality of HIT products. Screen shots, for example, are an essential component for learning best practices for EHR usability and performance, and some HIT developers have sought to prohibit the disclosure of such information and communications intended for knowledge sharing. **The AAMC supports this proposal and believes that ONC has struck the appropriate balance between ensuring that**

stakeholders who use and work with HIT can openly discuss and share experiences and information about HIT performance and protecting the legitimate intellectual property rights of HIT developers.

Maintenance of Certification Requirements

ONC proposes requiring HIT developers to issue a written notice to all customers within six months of the effective date of the final rule that any contravening communications of contract provisions regarding communication will not be enforced. Such notice would be required annually, until the developer has amended the contract to remove or void the offending language, which developers would have two years from the effective date of the final rule to complete. **The AAMC supports this proposal and suggests that ONC clarify that the amendment of these specific provisions should not be used inappropriately as an opportunity to amend or renegotiate other contract terms.**

Application Programming Interfaces (APIs)

In the proposed rule, ONC expresses its desire to ensure that patients have access to their own health information through the use of apps. While we support patient access to information, we are concerned that a patient may not understand that their information obtained through apps may be shared with third parties that are under no obligation to keep that information private. Health information is very personal and there is a potential for the information shared in apps to be used in ways that impact employment, access to affordable health insurance, or other areas.

As proposed, ONC would require that health information be shared through apps; yet they do not establish any patient privacy and security protections or any standards regarding how the information from the app may be used. Before finalizing these rules, patients and policymakers should have a comprehensive dialogue regarding the potential consequences of the impact of using apps and develop approaches that protect a patient's privacy and security. Patients and consumers should have access to better information and tools to assess apps with which they will share their health data. They also should understand what rights and protections they have for their private health data when they choose to share it through an app.

Approaches could include requiring EHR API vendors that are certified by ONC to certify that the apps meet established best practices and privacy guidelines and to provide a model notice to patients regarding how their information might be used by the app. Labeling is an approach that could be used to enable patients to better understand the security of a given app. ONC and CMS should consider leading an effort for such a labeling standard or could partner with a non-governmental entity to maintain a labeling system. For example, ONC could look to the Patient Privacy Rights group's "Information Governance Label" as an example of a check list for assessing an application's information security.¹ **Patients and consumers should have access to better information and tools to assess apps to share their health data with, and should understand what rights and protections they have for their private health data when they choose to share it through an app.** ONC should consider extending protection of the patient's health data privacy to include these third parties.

¹ Patient Privacy Rights (PPR) "Information Governance Label" available at https://docs.google.com/document/d/1-62rk2oN_BYop7Vag1cLbEmAybeJ_cgpn2e07BH8_bM/edit (last visited April 30, 2019)

Proposed API Standards, Implementation Specifications, and Certification Criterion

ONC is proposing to adopt standards, implementation specifications, and a new API certification criterion as part of its efforts to implement the Cures Act. Specifically, the Cures Act requires HIT 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[.]” The law also states that a developer must, through an API, “provide access to all data elements of a patient’s electronic health record to the extent permissible under applicable privacy laws.” ONC is proposing that “without special effort” means that HIT developers seeking certification must have the following three attributes: standardization of technical capabilities, transparency of business and technical documentation that is publicly accessible, and pro-competitive business practices that do not interfere with a provider’s use of their acquired API technology.

The proposed new API certification criterion would require FHIR servers to support API-enabled services for two types of data requests. The first would support a single patient’s data interaction with software applications controlled and used by a patient as well as software applications implemented by a provider to enhance clinical care tools and workflow. The second would support multiple patients’ data (“population-level”) interaction with software applications used by providers to manage internal patient populations in addition to external services to support a provider’s quality improvement, population health management, and cost accountability vis-à-vis health plans and other partners.

The AAMC supports standardization and transparency associated with APIs so long as protections are in place to promote the privacy and security of EHI.

Adoption of FHIR Standard [§ 170.215(a)(1)]

In terms of specific API standards, ONC proposes to adopt the HL7® Fast Healthcare Interoperability Resources (FHIR) Standard as a foundational standard. ONC estimates that 87% of hospitals and 57% of clinicians are served by HIT developers with a FHIR Release 2 API (and that 69% of clinicians are served by developers with any version an FHIR API). ONC goes on to say that FHIR Release 3 is not in widespread use, but that Release 4’s improvements are such that ONC is the standard that the industry would coalesce behind. **The AAMC supports a regulatory approach that allows the time necessary for the industry to adopt and implement Release 4, while maintaining certification under Release 2 in the interim.** Under this approach, ONC could then, when appropriate, add a maintenance of certification requirement to establish an upgrade timeframe to the FHIR Release 4 for HIT developers initially certified under Release 2.

Transparency Conditions [§ 170.404(a)(2)]

ONC proposes to permit API Technology Suppliers to institute a process to verify the authenticity of application developers so long as such process is objective and the same for application developers and completed within five business days of receipt of an application developer’s request to register their software application for use with the API Technology Supplier’s API technology. ONC is clear in the text of the proposed rule that applications (apps) would not have unfettered access to a health care provider’s data once connected to it through the API technology, and that an API Technology

Supplier or health care provider could de-activate the application's access if the application developer behaves in anomalous or malicious ways. Additionally, ONC is clear that patients will have to authenticate themselves, authorize the app to connect to the FHIR server and specify the scope of data which the app may access when a patient seeks to access his or her data using an app.

The AAMC supports the proposal to permit an authenticity verification but urges ONC to consider a longer timeframe to complete the verification process and additional vetting of application developers. The AAMC is concerned that the five-business day turnaround to verify the authenticity of application developers may not be enough time for API Technology Suppliers to authenticate application developers, especially during the initial sprint after the rule is finalized. The AAMC urges ONC to adopt a longer verification turnaround timeline of at least ten business days and revise the standard after evaluating the real-world experience of API Technology Suppliers in authenticating developers.

Permitted Fees Conditions [§ 170.404(a)(3)]

Generally, API Technology Suppliers will be prohibited from imposing any fees under ONC's proposal, but certain permitted fees will be allowed. The permitted fees are intended to recognize that Suppliers need to recover costs and earn a reasonable return for providing certified API technology. ONC proposes general conditions for permitted fees in addition to satisfying one of the specific proposed permitted fees.

There are four general conditions on permitted fees. First, the fee must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. Second, fees imposed must be reasonably related to the Supplier's costs of supplying and supporting API technology to the user being charged (e.g., a Supplier could not charge a fee if the underlying costs had already been recovered). Third, the costs to supply and support the API technology for which the fee is based must be reasonably allocated among all the Supplier's customers using the technology. And finally, fees cannot be based in any part on whether the requestor or other party is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the Supplier.

The specific permitted fees are: (1) development, deployment, and upgrades; (2) supporting API uses for purposes other than patient access; and (3) value-added services. Except for value-added services, fees would always be between the Supplier and the API Data Provider, defined as the entity that deploys the API technology. Only value-added services fees could be charged API Users, defined as persons and entities that use or create software applications that interact with the APIs developers by the Supplier and deployed by the Data Provider.

The AAMC urges ONC to reconsider its proposals related to permitted fees, as they are likely to place significant financial burden on the API Data Providers. ONC should consider balancing the costs associated with API development and deployment across both API Data Providers and certain API Users, to ensure that third-party software application developers are contributing. Third-party app developers are likely to generate revenue from the use of their apps and mining the data that is shared, and thus should have some responsibility for paying fees. Placing any significant portion of the fee burden on providers is unfair, considering all of those in the marketplace who might benefit financially from open APIs.

INFORMATION BLOCKING

The Cures Act added a section (3022 of the Public Health Services Act) to define and prohibit information blocking by health care providers, IT developers of certified health IT, health information exchanges and health information networks. While section 3022 defines information blocking in broad terms, it also identifies activities that would not be considered information blocking, which are referred to as exceptions. To qualify for any of these exceptions, an individual or entity must satisfy *all* the applicable conditions of the exception. The burden of proof would be on the individual or entity to demonstrate compliance with all the conditions. ONC proposes that the information blocking requirements would be effective as of the date of the final rule.

Innocuous and Beneficial Activities Should Not be Considered Information Blocking

The AAMC supports efforts to deter practices that unnecessarily impede the flow of EHI or its use to improve health and the delivery of care. Making information available to providers and patients is an important step toward improving patient care. The information blocking provision as proposed would encompass a broad range of potential practices. We believe it is important that activities that are innocuous and beneficial (e.g. protecting patient privacy) are not considered violations of the information blocking provision.

To minimize burden for providers, the information blocking provisions and exceptions need to be clear, predictable, and feasible to implement. They must be sensitive to practical challenges that may prevent access, exchange, or use of EHI. It is critical to accommodate practices that may inhibit access exchange or use of EHI but are reasonable and necessary to advance other critical interests such as preventing harm to patients and others, promoting the privacy and security of EHI, and encouraging innovation.

Implementation Time Frame is Unrealistic

The AAMC has significant concerns that the effective date of the information blocking provisions included in the proposed rule is unrealistic. **ONC must provide sufficient time for actors to comply with the information blocking provisions after the rule is finalized.** As proposed, the information blocking provisions would go into effect long before the technology upgrades to facilitate EHI exchange are available. **At a minimum, we recommend no enforcement of the information blocking provisions for a period of 24 months after the effective date of the final rule.** Health care providers will need time for education and training about the new rules and to revise any organizational policies, guidelines, or contracts to comply with the rules.

ONC should also clarify that the information blocking requirements do not apply retroactively to providers. For example, a provider should not be considered an information blocker if there is a request for information from many years ago. For example, consider a provider who has a patient's data stored electronically in their EHR going back to 2017. That provider receives a request in 2021 for the patient's data back to 2017, but in the intervening years has not provided care to the patient. Satisfying such a request could be particularly difficult since the provider needs to obtain consent or authorization to release the patient's data that was entered in the EHR so long ago. We ask that ONC

clarify whether significant lags in time between the request for data and when care was provided and electronically documents meets any of the proposed exceptions or deserves its own exception.

Definitions

Providers Should Not be Included in Definition of Health Information Network (HIN) and Health Information Exchange (HIE):

ONC proposes to establish definitions of health care providers, health IT developers of certified health IT, health information exchanges, and health information networks to whom the information blocking provisions would apply. ONC seeks comments on the proposed definitions of these terms, particularly on whether the definitions are broad enough or too broad.

We have specific concerns with the definition of Health Information Networks or HINs, which ONC defines as an individual or entity that satisfies one or both of the following:

*Determines, oversees, administers, controls, or **substantially influences** policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.*

• *Provides, manages, controls, or **substantially influences** any technology or service that enables or facilitates the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.*

In the rule, CMS provides examples of health care providers that it would consider to be health information networks under this definition. We recommend that ONC change the proposed definition to clarify that a health care provider would not be considered a “health information network.”. Since health care providers are already considered “actors” that would be prohibited from information blocking, it is not necessary to include providers in the definition of health information networks and to subject providers to the steep penalties (up to \$1 million per violation) that would apply if they are included in the definition of health information networks. Adopting such a broad definition could discourage providers from participating in health information networks.

In addition, we recommend that the term “*substantially influences*” be removed from the definition as this could potentially result in the inclusion of entities that should not be considered health information networks.

ONC proposes to define the term “health information exchange” to mean an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes. ONC notes this would include regional health information organizations, state health information exchanges, and other types of organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used among particular types of parties or for particular purposes. We recommend that ONC clarify that health care providers are not considered “health information exchanges.” As mentioned in our comments above related to the definition of “health information networks,” the proposed definition is too broad and could discourage provider participation in health information exchanges.

The Electronic Health Information Definition is Overly Expansive and Should Be Revised to USCDI Data Elements Stored Within the EHR

A foundational part of this rule is the definition of “electronic health information” (EHI) to which the information blocking rules apply. In this rule, ONC proposes to define EHI as 1) electronic protected health information; and 2) any other information that is transmitted by or maintained in electronic media, identifies the individual or can be used to identify the 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.

ONC seeks comment on the proposed definition of EHI. **The AAMC believes that this definition includes an overly expansive set of information, and the technology is not in place at this time for the inclusion of this amount of information. Instead, we recommend that ONC define EHI as the United States Core Data for Interoperability (USCDI) data elements, which includes a standardized set of data classes and data elements, that are stored in a provider’s EHR.** This definition would be consistent with ONC’s proposal to adopt USCDI as the data elements that would be required to support nationwide electronic health information exchange under the certification program.

Price Information Should Not be Included in the Definition of EHI

ONC mentions in the proposed rule that the definition of EHI would “include information on ...billing for health care services and payment information for services to be provided or already provided, which may include price information.” ONC seeks specific comments on the parameters and implications of including price information within the scope of EHI for purposes of information blocking. In addition, it seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

The AAMC supports efforts to ensure consumers have information concerning their cost sharing obligations; however, **we oppose the inclusion of price information in the definition of EHI that applies to information blocking. While we recognize the importance of patients having information regarding the cost of their care, there is a need to carefully consider the best approach to providing patients with the type of information needed to understand their potential cost-sharing responsibilities. Inclusion of pricing information in the definition of EHI is not the appropriate avenue for achieving this goal.** Pricing information is not readily available in EHRs currently and providers often do not have access to this information.

Many challenges must be overcome to provide accurate price information to patients. Out-of-pocket cost information is the most relevant pricing information for patients. A patient’s cost-sharing obligation is determined based on the benefits and coverage under a specific insurance plan, the plan’s provider network and cost-sharing structure, and the negotiated rates between the plan and provider.

For patients it is also difficult to get a clear assessment of the cost of services due to the nature of health care. The path to diagnosis and treatment can vary significantly for each individual and there are many variables that will impact the cost, making it very difficult for providers to produce cost

estimates. Over the course of an episode of care, the patient may see multiple providers and seeking price information separately from each provider may not give the patient accurate information about the cost of care.

Payers are better positioned to provide cost-sharing information to their beneficiaries and plan enrollees. The payers can provide information about limitations on coverage, deductibles and coinsurance. In addition, a payer can provide more information across the entire episode of care involving multiple providers. If the patients do not understand the price information, there may be unintended consequences, such as patients forgoing medically necessary care if they perceive the cost to be too high (even if the price is not actually what the patient would pay out of pocket). Also, patients also need to factor in other considerations, such as the quality of care, in order to evaluate the price. As discussed above, price information is very difficult to provide in a way that is meaningful to patients who are most concerned with their out of pocket cost. While we agree that improvements should be made regarding price transparency, we do not think defining price information within the definition of EHI would be beneficial to patients and could result in unintended negative consequences.

Observational and Non-Observational Data

ONC acknowledges in the rule that the proposed definition of EHI would include observational health information and non-observational health information. ONC expresses concerns with information blocking that would interfere with access to observational health information, which would include health information about a patient that could be captured in a patient record within an EHR or other system when the information is clinically relevant, directly supports patient care, or facilitates the delivery of health care services. (e.g., lab test results). In contrast, non-observational information would include information that is created through aggregation, algorithms, and other techniques that transform observational health information into fundamentally new data or insights that are not obvious from the observational information alone. Examples would include population-level trends, predictive analytics, risk scores and EHI used for comparisons and benchmarking activities, or internally developed quality measures.

The AAMC supports the inclusion of observational health information within the definition of EHI. It is important to ensure that health care professionals have timely access to the “observational information” they need to make treatment decisions and effectively coordinate and manage their patient’s care. **However, we oppose the inclusion of non-observational information within the definition of EHI to which the information blocking provision applies. Inclusion of this type of information is not necessary for direct patient care and could potentially deter reporting of adverse events and quality improvement initiatives.** Non-observational information could be utilized for quality improvement purposes and may not be generalizable or interpretable beyond the particular health care encounter or setting. Also, providers may be discouraged from reporting adverse events in the EHR due to concerns that this information would be used against the provider. Providers may fear reporting quality information due to concerns with how this information may be used. ONC should carefully consider unintended consequences of including non-observational information and the chilling effects its inclusion might have on quality and safety initiatives.

Exceptions for Activities that Do Not Constitute Information Blocking

ONC details examples of what constitutes information blocking and proposes seven exceptions to the information blocking provision that would apply to certain activities that may technically meet the definition of information blocking but that are reasonable and necessary to further the underlying public policies of the information blocking provision. To qualify for any of these exceptions, an individual or entity must satisfy *all the applicable conditions* of the exception. The burden of proof would be on the individual or entity to demonstrate compliance with all the conditions. ONC invites comment on the types of documentation and/or standardized methods that an actor may use to demonstrate compliance with the exception conditions.

We are pleased that ONC has expressed its commitment to reduce unnecessary documentation and reporting burdens. However, we are concerned that the requirements associated with meeting the exceptions for the proposed information blocking provisions could result in greater burden and cost to providers. Understanding how the complex information blocking provisions will impact daily practice is very complicated.

The AAMC is concerned about the significant burden and cost placed on providers to prove that they meet the information blocking exceptions. The definitions of terms are broad and ambiguous, which can make it difficult for providers to know if they are complying with the rule. As described in the proposed rule, providers would be required to meet extensive documentation requirements to demonstrate that they have met the criteria in the exception for information blocking. **We recommend that ONC give examples and guidance on the exceptions and the type of documentation that would be acceptable to support the criteria. We recommend that ONC review this requirement with an eye towards reducing regulatory burden reduction.**

We also recommend that rather than putting the entire burden on the provider, standards be established for the requestor of the information. At a minimum, the requestor should specify what information they are requesting, delineate the reason for requesting the information, and provide some background information about who they are.

Exception: Preventing Harm

ONC proposes an exception to information blocking for reasonable and necessary practices to prevent harm to a patient or another person, subject to certain conditions which must be met at all relevant times. The likelihood of harm to a patient or other person can result from corrupt data in the EHR, misidentification of EHI, or disclosure of information that could endanger the life or safety of the patient. ONC states that the actor can implement an organizational policy or make a finding in each case based on the facts and circumstances. In this exception, ONC states that if a provider has identified a piece of information that had been misattributed to the patient, the provider would not be excused from exchanging or providing access to all the other EHI about the patient in the record.

We support the categories of harm described in the preventing harm exception. In these circumstances, it is appropriate for the provider to restrict access, exchange or use of PHI in to certain requestors to protect the patient's safety. However, we are concerned about requiring the provider to exchange the remainder of the EHI in the record that does not pose a risk to safety. While we understand the need to share information, it is very difficult with the existing technology to

extract portions of the medical record that are “sensitive” or pose safety risks and to provide the remainder of the record. Providers are currently working toward achieving the ability to “tag” and separate parts of the record. Until this technology is implemented, the segmentation of the EHI could be very difficult to achieve.

Exception: Promoting the Privacy of EHI

Information Blocking Rules Must be Aligned with HIPAA Privacy and State Privacy Laws to the Extent Possible

ONC proposes an exception to protect the privacy of an individual’s EHI. ONC notes that any privacy protection practice must be consistent with applicable laws related to health information privacy, such as the HIPAA Privacy Rule, the HITECH Act, and state privacy laws. ONC acknowledges that its information blocking rule may require actors to provide access, exchange or use EHI in situations where HIPAA does not. HIPAA permits covered entities to use and disclose ePHI for treatment, payment, and healthcare operations; the information blocking rule requires actors to provide access, to exchange, or to use EHI unless they are prohibited from doing so under federal or state law or are covered by one of the proposed exceptions. ONC proposes 4 sub-exceptions for promoting privacy.

We are concerned that the intersection with existing Health Insurance Portability and Accountability Act (HIPAA) regulations is complicated and providers will need time to understand the implications in daily practice. The information blocking rule creates potentially conflicting requirements on providers under the Health Insurance Portability and Accounting Act (HIPAA) and Substance Abuse Confidentiality Regulations (42 CFR Part 2 regulations). As a result, clinicians will be unclear about what information they are permitted verses required to share. **To the extent possible, these federal programs and state policies need to be aligned to reduce burden and confusion prior to implementation.**

As an example, ONC information blocking proposal, which requires a physician to disclose all EHI if requested (unless an exception applies) conflicts with HIPAA’s minimum necessary requirement. It may be difficult for physicians to understand whether applying the minimum necessary standard fits into an exception. Some clinicians may find it easier to simply disclose all the information they have rather than taking on the risk that they may be identified as an information blocker. ONC should clarify that physicians providing the minimum necessary information to a requestor will not be considered an information blocker, without having to take steps to meet requirements of the relevant Privacy sub-exception.

Sub-Exception: Precondition Imposed by Law not Satisfied

This exception would protect actors that choose not to provide access, exchange, or use of EHI when a state or federal privacy law requires the actor to satisfy a precondition and that precondition has not been satisfied (e.g., no consent or authorization). ONC proposes that for preconditions that rely on the provision of consent or authorization from an individual, the actor must have *done all things reasonably necessary* within its control to provide the individual with a meaningful opportunity to provide the consent or authorization and must not have improperly encouraged or induced the individual to not provide the consent or authorization.

The AAMC supports this sub-exception. Providers should not be compelled to share EHI without adequate safeguards out of concern that restricting access, exchange, and use of that information would be information blocking. If they are forced to release this information, the patients' trust and confidence in the privacy of their information would be undermined and they would be less willing to share information electronically. Personal privacy rights and concerns for inappropriate or rogue parties who attempt to gain advantage with health care information must be balanced and not suppressed by the need for interoperability.

ONC sets forth conditions, including provision of a meaningful opportunity to consent, based on its assumption that providers may use the protection of an individual's privacy as a pretext for information blocking. Rather than assuming bad intent, ONC should recognize that meeting certain preconditions may be outside the direct control of the provider. For example, the provider may have a very difficult time tracking down a former patient and obtaining an authorization or consent to disclose the information. **If "meaningful opportunity" is defined too broadly the burden on the provider to provide a "meaningful opportunity for the beneficiary to provide consent or authorization" could be significant. If the patient is not present in the office to provide consent, we recommend that it would be reasonable for the provider to obtain the consent the next time the patient visits the office. In addition, the burden to obtain the consent should be on the organization requesting the data rather than the organization that holds the data.** However, providers would need assurances that consents are legitimate and are in their possession before sharing any data.

ONC seeks comment on how this proposed sub-exception would be exercised by actors in the context of state laws. They are aware that actors that operate across state lines or in multiple jurisdictions sometimes adopt organization-wide privacy practices that conform with the most restrictive privacy laws. ONC is considering the inclusion of an accommodation in this exception that would recognize and actor's observance of a legal precondition that the actor is required by law to satisfy in at least one state in which it operates. We support making this accommodation as this would ease the burden for health care systems that operate in multiple states.

Exception: Promoting the Security of EHI

ONC proposes an exception to permit actors to engage in reasonable and necessary practices to promote the security of EHI. ONC notes that a practice that complies with the HIPAA Security Rule might not necessarily qualify for this proposed exception. To qualify for this exception, ONC proposes that an actor's conduct must satisfy threshold conditions: 1) the security-related practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI; 2) implemented consistently in a nondiscriminatory manner and tailored to identified security risks.

We recommend that ONC clarify that this exception allows providers to be proactive when promoting the security of electronic health information rather than taking a reactive stance. For example, the standard should not require that the provider respond to a "known security threat or incident" in order to meet the requirements of the information blocking exception for security. Health care providers and developers must be vigilant to mitigate security risks that have been escalating in recent years and implement appropriate safeguards to the secure the EHI they collect and exchange.

ONC states that the actor's organizational policy on security must align with one or more consensus-based standards or best practice guidance. This could be a difficult standard to meet since there are many emerging security threats that occur that are new and unexpected. For these novel threats, consensus-based standards and best practice guidance may not exist, making it impossible for a provider to meet the requirement that the organizational security policy align with such standards.

Exception: Responding to Requests that are Infeasible

ONC notes that in certain circumstances there are legitimate practical challenges beyond an actor's control which limit its ability to comply with requests for that access, exchange or use either because they may not have the technological capabilities, legal rights, financial resources, or other means necessary to provide a particular form of access, exchange or use, or they would incur costs that are clearly unreasonable. To receive this protection the actor must demonstrate complying would impose a substantial burden that is unreasonable under the circumstances, timely respond to the request, provide the requestor with a detailed written explanation of why they cannot accommodate the request, and work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging or using the EHI.

In general, we support this exception and appreciate the recognition that there may be practical challenges beyond a providers control. However, we are concerned with the burden this requirement places on the provider to identify reasonable alternative means of accessing, exchanging or using the EHI as well as the necessary documentation. We recommend that ONC provide additional clarification on how extensive an effort the provider would need to make to come up with alternatives and the documentation needed to support the exception.

Exception for Complying with Common Agreement for Trusted Exchange

ONC is considering whether to propose in future rulemaking a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement for Trusted Exchange. We support this exception as we believe it will support adoption of the Common Agreement and encourage other entities to participate in trusted exchange through HINs.

Disincentives for Health Care Providers: Request for Information

A provision in the PHSA provides that any health care provider determined by the OIG to have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives. Establishing harsh disincentives for providers when implementing a complex new set of requirements may shift the behavior incentives from appropriately preventing harm to a patient and protecting and managing their confidential health information to avoiding penalties for the individual and/or the organization. These requirements will take several years to understand their full scope and we will learn of unexpected and unanticipated complications. ONC requests information on disincentives to deter information blocking. For providers, there are already substantial disincentives to information blocking in the Promoting Interoperability Program. Hospitals that taken any action to limit or restrict interoperability or exchange of information face hefty financial penalties under the inpatient PPS and CAH programs. They would be subject to a 75% reduction to the IPPS market basket update applied to Medicare Part A reimbursement under the

inpatient Prospective Payment System (IPPS) payment system. In the MIPS program, eligible clinicians' performance scores and resulting payment will also be negatively impacted if they are identified as "information blockers." Therefore, there is no need to establish other disincentives since the Promoting Interoperability Programs for hospitals and eligible clinicians already contains substantial disincentives.

PATIENT MATCHING REQUEST FOR INFORMATION

Achieving interoperability and information sharing will require the ability to match a patient's data across health settings and HIT systems accurately. ONC appropriately notes that accurate and standardized data capture and exchange optimized algorithm performance are critical components to accurate patient matching. Unfortunately, patient matching rates vary widely.² Patient matching is a quality of care and patient safety issue because inaccurate patient matching can lead to inappropriate, potentially risky, and unnecessary care. Also, correction of misidentification is burdensome on both patients and providers. Errors introduced into a record by inappropriate matching may live on due to cutting and pasting information. While misidentification is a critical error that providers should be able to easily correct, current systems are not in place that easily enable correction of matching errors. **The AAMC appreciates ONC's request for information on creative, innovative, and effective approaches to patient matching within and across providers. Progress on patient matching is critical to EHR interoperability and helping patients receive appropriate and needed care when they seek it.**

Providers, software developers, and other healthcare organizations should collaborate on the identification of a common set of data elements that should be collected by providers using federally adopted standards to support patient matching. While we recognize that there is a current ban on the federal government's ability to develop a unique patient identifier, we believe that HHS can collaborate and provide technical assistance to the private sector in developing and testing standards for patient matching.

Data Collection Standards and Other Solutions to Improve Accurate Data Capture

A recent study by experts from Indiana University and supported by The Pew Charitable Trusts found that the standardization of patient addresses using the United States Postal Service's format showed promise for improving the success of a matching algorithm.³ **ONC should consider steps it could take to improve standardization of address data**, including updating policies that govern how digital systems exchange information to support use of the Postal Service format or coordinating use of the Postal Service's address validation API (used by the shipping industry to improve the delivery of mail and packages) for use in the healthcare sector to improve patient matching.⁴

² Patient Identification and Matching Final Report, February 7, 2014. Available at:

https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf

³ Shaun J Grannis, et al., *Evaluating the effect of data standardization and validation on patient matching accuracy*, JAMIA. March 8, 2019. Retrieved from: <https://academic.oup.com/jamia/article-abstract/26/5/447/5372371>.

⁴ United States Postal Service, "Address Information API," documentation available at <https://www.usps.com/business/web-tools-apis/address-information-api.htm> (last visited May 2, 2019).

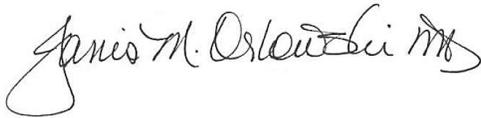
Data Elements to Assist in Patient Matching

Similarly, as more and more demographic data elements are captured in the EHR, ONC should examine studies to look at whether these elements could be used to improve patient matching. For example, it is believed that more than half of patient records include an electronic mail (e-mail) address and mother's maiden name. If these elements are already in the EHR, they should be used for patient matching. E-mail in particular could be a promising additional element for matching, as it is collected more and more in an effort to provide patient access to patient-facing records portals.

Conclusion

The AAMC welcomes engagement on these issues and appreciates the opportunity to comment. We look forward to continuing work with ONC on these issues. If you have any questions, please contact Gayle Lee at (202) 741-6429 or galee@aamc.org and Phoebe Ramsey at (202) 448-6636 or pramsey@aamc.org.

Sincerely,



Janis M. Orlowski, M.D., M.A.C.P.
Chief Health Care Officer

cc: Ivy Baer, AAMC
Gayle Lee, AAMC
Phoebe Ramsey, AAMC
Keith Horvath, AAMC