May 31, 2019

Don Rucker, M.D.
National Coordinator for Health Information Technology
Office of the National Coordinator
U.S. Department of Health and Human Services
330 C ST SW
Mary Switzer Building; Mail Stop 7033A
Washington, D.C. 20201

Re: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (RIN 0955-AA01)

Submitted electronically

Dear Doctor Rucker:

Carequality is pleased to submit comments to the Office of the National Coordinator for Health Information Technology (ONC) on the proposed rule *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program.* We appreciate ONC's demonstrated commitment to consider thoughtfully the comments that it receives from stakeholders in response to such proposed rules.

Carequality is a non-profit, 501(c)(3) organization that provides a national-level, consensus-driven, interoperability framework to enable exchange between and among health data sharing networks and stakeholders. While The Sequoia Project was previously the corporate home for Carequality, Carequality now operates as a separate non-profit corporation.

Carequality supports the exchange of over 19 million clinical documents each month, involving approximately 600,000 care providers, 40,000 clinics, and 1,400 hospitals. To do so, it brings together a diverse group of representatives, including many types of provider organizations, electronic health record (EHR) developers, payers, health information exchanges, consumer applications, interoperability service providers, and government agencies. These stakeholder representatives collaborate in an open forum to maintain the technical and policy agreements that enable data to flow between and among networks, platforms, and geographies, much like the telecommunications industry did for linking cell phone networks.

Enabling such widespread connectivity, without individual pre-coordination with each partner, requires three core elements: common rules of the road, well-defined technical specifications, and operational components including a participant directory and digital certificates. Carequality has implemented each of these pieces, and provides a practical, operational framework for connecting the country through existing networks. The comprehensive Carequality Interoperability Framework consists of multiple elements, including legal terms, policy requirements, technical specifications, and governance processes, which operationalize data sharing under established Principles of Trust. The Framework is

available for health information exchange networks, vendors, payers, and others across the healthcare ecosystem to adopt, and provides a practical approach to unlocking previously unseen levels of connectivity. In addition to the existing live exchange of clinical documents, Carequality has active workgroups extending the Framework to support and facilitate exchange using HL7 FHIR, and enabling an ecosystem for pushed notifications, including but not limited to ADT event notifications.

Our comments are based on our experience developing and operating the Carequality Framework. Via this work, we have gained both a wealth of operational experience in the practical implementation of health information exchange on a nationwide scale and have become an experienced, technically expert, transparent and neutral convener of public and private-sector stakeholders to address and resolve practical challenges to interoperability through the Carequality Framework.

Overview

Carequality supports the congressional intent of the 21st Century Cures legislation for greater data liquidity. We appreciate the care with which ONC approached its implementation responsibilities. Our detailed comments are in the attached Appendix. Overall:

- Carequality generally supports ONC's approach to open Application Programming Interfaces (APIs) and the specification of several standards, including HL7® FHIR®. Of the ONC's options for the version of FHIR® and associated standards for the final rule, we strongly support Option #4—FHIR® Release 4 (or the latest balloted version of FHIR®). Note that, for FHIR® Release 4, the applicable implementation guide would be US Core STU 3.1.0, which is expected to be published late 2019.

- We ask ONC to emphasize that the proposed initial set of FHIR resources to be used with the proposed API, the *API Resource Collection in Health* (ARCH), is always bounded by the scope of the US Core Data for Interoperability (USCDI), that the USCDI will only include data classes and data elements that have SDO-developed implementation guides, that the ARCH will only reference HL7® FHIR® resources, and, moving forward, the function of the ARCH is transitioned as rapidly as possible to a private sector, SDO-developed implementation specification, such as the HL7® US Core.

- We urge ONC to take careful heed of comments from providers and developers on the practicality and reasonableness of its proposed timelines and the burdens that these timelines could create, both from the standpoint of technology development and implementation and the need for development and implementation of complex new organizational policies.

- We urge ONC to also recognize the need for flexibility for providers and developers and the need to set realistic expectations for the proposed expanded data export functionality; we encourage ONC to consider carefully feedback from the developer community on the potential challenges and cost associated with this proposed criterion.

- On information blocking, we commend to ONC the comments of the Sequoia Project on this issue as well as the work of the Information Blocking Workgroup of The Sequoia Project's Interoperability Matters Cooperative, attached as Appendix 2. I had the honor of representing

Carequality on this workgroup.

Although much of ONC's focus is identification of "reasonable and necessary" activities that may interfere with the access, exchange, or use of electronic health information (EHI) but do not constitute information blocking, the proposed practices, definitions, and the other regulatory and sub-regulatory discussions and provisions, will also have a substantial impact on implementation of this rule.

- In particular, the proposed definitions of "access," "exchange," "use," and "electronic health information" (EHI) are very broad. These will interact with each other, with ONC's definitions of the four actors, with the rule's descriptions of information blocking practices, and with the seven proposed exceptions. The result is an extensive and diverse set of scenarios and use cases that will be subject to complex compliance and enforcement. The impact, foreseen and unforeseen, may exceed and even be inconsistent with Congress' intent to define and limit information blocking.

- We are especially concerned with the implications of the very broad definition of EHI and the likely impracticality of applying the information blocking provisions to this extensive, highly situational and largely non-standardized data set. We suggest that enforcement focus most heavily on assuring access to the USCDI (including API access), which will evolve over time to include more and more EHI. We pledge to work closely with the community and ONC to achieve this goal.

- One area of great importance to Carequality is the definition of "Health Information Exchanges" and "Health Information Networks". We believe that the distinctions between these two categories are unclear and the definitions too broad (especially for HINs) and could sweep in organizations (e.g., provider organizations, and SDOs and similar organizations) that would otherwise not have liability for the very high fines applicable to HIEs and HINs. These definitions could similarly subject a broad array of organizations to the very stringent requirements (e.g., on pricing and licensing) associated with the exceptions relevant to these actors.

- Overall, we believe that the seven categories of "reasonable and necessary" exceptions are the correct ones and indeed, are essential to practical implementation of the information blocking prohibition.

- With respect to the exceptions, however, we have concerns and questions about specific elements. We especially highlight our concern with the proposed requirement that "[t]o qualify for any of these exceptions, an individual or entity would, for each relevant practice and at all relevant times, must satisfy all applicable conditions of the exception". Such a strict compliance standard may add clarity, but it is at odds with the complexity that underlies healthcare operations, for example in responding to complex security threats, and may inadvertently penalize many individuals and organizations who are acting in good faith as it seeks to identify or deter a relatively few "bad actors". We also have concerns with the costs that will result from organizations needing to manage these complex policies and document their actions. We comment selectively on this in Appendix 1.

- In addition, we ask ONC to clarify that requiring compliance with a trust framework (or HIN agreement, more broadly) is not information blocking, even if there is another plausible or even reasonable way to accomplish the same effect. One example would be if an organization (e.g., an HIE or HIN) has a policy that its participants cannot condition their provision of information on the recipient paying a fee for certain use cases or permitted purposes, such as treatment (i.e., an HIE or HIN would be permitted to prohibit charging certain types of fees under specific circumstances without that policy implicating information blocking).

- Similarly, we believe that ONC should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices necessary to comply with the requirements of the Common Agreement (TEFCA). We believe that ONC should broaden this exception to include compliance with the terms of private sector trust frameworks whose aim is to enhance interoperability. As indicated above, we urge that ONC explicitly indicate that such trusted exchange frameworks can design and implement agreements that impose specific obligations on participants, and that they can employ specific provisions intended to gain participation and hence, to enable greater flow of EHI. We also ask ONC to be clear that such frameworks can choose, and HINs more generally can choose, to focus on specific EHI-exchange use cases and not to address others, potentially subject to a minimum floor as discussed above.

- Finally, we comment on the Patient Matching Request for Information. We agree with ONC on the importance of this issue and of the role of the private sector, with federal government support, in improving match rates. We point ONC to the Sequoia Project's "A Framework for Cross-Organizational Patient Identity Management," first published in 2016 and updated in 2018.[1] We especially emphasize that much of the focus in accurate patient matching has been intra-organizational but that true interoperability and data liquidity will require accurate cross-organizational matching.

Conclusions

We thank ONC for providing the opportunity to comment on this proposed rule. Carequality is eager to assist ONC in advancing our national interoperability agenda.

Respectfully,

Dave Cassel
Executive Director, Carequality

[1] https://sequoiaproject.org/resources/patient-matching/

Appendix 1: Specific Recommendations and Comments

IV.B. Revised and New 2015 Edition Criteria

1. The United States Core Data for Interoperability Standard (USCDI) (p. 7440)

ONC proposes to remove the Common Clinical Data Set (CCDS) from the 2015 Edition of certification criteria and replace it with the United States Core Data for Interoperability (USCDI) Version 1. To achieve the goals set forth in the Cures Act, ONC intends to establish and follow a predictable, transparent, and collaborative process to expand the USCDI as well as flexibility for developers to certify to newer versions of standards that have been approved by the National Coordinator through the Standards Version Advancement Process for use in certification.

Comment: We support ONC's proposal for the USCDI Version 1, the process for its updating over time, as well as the proposed Standards Version Advancement Process. We also support ONC's proposal that required USCDI development and implementation will be a specified multi-month period after the effective date of the final rule as well as the ability for earlier implementation of the USCDI by developers and providers when they are able to do so. At the same time, we urge ONC to be mindful and explicit that its proposed 24-month period covers both development and provider implementation, as do other instances of 24-month implementation timing for changes to the 2015 certification criteria. We urge ONC to give serious consideration to comments from providers and developers on the timeline implications and make any needed adjustments to this aggressive proposed timeframe based on this feedback.

In general, we agree with the specific elements of Version 1, including addition of Clinical Notes as a Data Class, the initial set of note types selected, and ONC's stated intention to expand this list over time. With respect to clinical notes, we draw ONC's attention to a 2018 joint Carequality/CommonWell document "Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes, February 2019 [2]. This white paper defines a path to improve the content in C-CDA® exchange, including recommendations for including notes in C-CDA®s.

4. Electronic Health Information Export (p. 7446)

ONC proposes a new 2015 Edition certification criterion for "electronic health information (EHI) export" that would replace the 2015 Edition "data export" certification criterion. 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, and (2) support the export of EHI when a health care provider chooses to transition or migrate information to another health IT system.

Comment: We agree with ONC's stated flexibility in seeking to allow developers to have the ability to create "innovative export capabilities according to their systems and data practices" and that ONC does not propose to require use of a specific export standard. We do, however, caution ONC to be realistic in its expectations and those it conveys to stakeholders regarding the goal to "provide patients and health IT users, including providers, a means to efficiently export the entire electronic

[2] https://s3.amazonaws.com/ceq-project/wp-content/uploads/2019/04/11013830/20190201_Improve_C-CDA_Joint_Content_WG_IHE_v1.1_Final.pdf

health record for a single patient or all patients in a computable, electronic format". Based on our experience, we have concerns that the nature of the exports available, given disparate EHR system architectures, will often fall short of this laudable goal and that the work required to implement this revised export criterion will divert from other priority interoperability goals that may be more achievable. We further note that HL7® interfaces and other interoperability tools are often used as conversion mechanisms. The more we improve the breadth and standardization of FHIR®-based APIs focused on the USCDI as it expands, the more reasonable they will be as future conversion mechanisms, reducing perceived need for separate export tools.

5. Application Programming Interfaces (APIs) (p. 7449)

ONC proposes to adopt a new API criterion to replace the "application access – data category request" certification criterion and become part of the 2015 Edition Base EHR definition. This new "standardized API for patient and population services" certification criterion would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications. The new criterion would focus on supporting two types of API-enabled services: (1) services for which a single patient's data is the focus and (2) services for which multiple patients' data are the focus. ONC proposes that certified health IT would need to be updated/implemented to this new criterion within 24 months of the effective date of the final rule.

Comment: We support this provision, and as addressed below, believe that of the four HL7® FHIR® standards options presented in VII.B.4, ONC should select Option #4—designation of FHIR® Release 4 (or the latest balloted version of FHIR®) in the final rule.

We also support ONC's proposal that required USCDI development and implementation will be a specified multi-month period after the effective date of the final rule as well as the ability for earlier implementation of the USCDI by developers and providers when they are able to do so. At the same time, we urge ONC to be mindful and explicit that this 24-month period includes both development and provider implementation, as do other instances of 24-month implementations timing for changes to the 2015 certification criteria. We urge ONC to give serious consideration to comments from providers and developers on the timeline implications and make any needed adjustments to this aggressive proposed timeframe based on this feedback.

7. Data Segmentation for Privacy and Consent Management Criteria

In the 2015 Edition, ONC adopted two "data segmentation for privacy" (DS4P) certification criteria, one for creating a summary record according to the DS4P standard and one for receiving a summary record according to this standard. Certification to the 2015 Edition DS4P criteria focus on data segmentation at the document level and is not required to meet the Certified EHR Technology definition (CEHRT) or required by any other HHS program. ONC proposes to remove the current 2015 Edition DS4P criteria and replace these two criteria with three new 2015 Edition "DS4P" certification criteria (two for C-CDA® and one for a FHIR®-based API) that would support a more granular approach to privacy tagging data consent management for health information exchange supported by either the C-CDA®- or FHIR®-based exchange standards.

Comment: Although we agree with and support ONC's intentions, we have some concerns about the practicality of these criteria, in part due to the burden for providers and developers, and the extent to which they will be used by developers and providers. We note that ONC's ISA shows a low adoption level of the current HL7® implementation guide published in May 2014 and the Consent2Share FHIR® Consent Profile Design is a new emerging standard in pilot with feedback requested.[3] We also understand that Consent2Share does not appear to have a clear owner moving forward and is not a standard nor implementation guide that has gone through an SDO process.

We also highlight the likely increased complexity involved in trying to enable certain data in the record to be carved out from sharing; for example, when information to be excluded may be in both structured data and notes. We also urge ONC to be mindful of setting realistic patient expectations for what such a standard and capability can achieve. For example, without fundamental and resource intensive re-architecting of existing EHR systems, clinicians who review the remainder of the record usually will be able to ascertain that something has been redacted, and often will be able to ascertain what it was.

VII. Conditions and Maintenance of Certification

ONC proposes to establish Conditions and Maintenance of Certification requirements for health IT developers based on the conditions and maintenance of certification requirements outlined in section 4002 of the Cures Act.

B.4. Application Programming Interfaces (APIs)

The Cures Act's API Condition of Certification include new standards, new implementation specifications, and a new certification criterion, as well as detailed Conditions and Maintenance of Certification requirements.

Comment: Carequality generally supports this provision and the proposed specification of several standards, including HL7® FHIR®. Of the options ONC outlines for the version of FHIR® and associated standards that should be specified in the final rule, we strongly support, for the reasons articulated by ONC, Option #4—designation of FHIR® Release 4 (or the latest balloted version of FHIR®) in the final rule.

Note that, for FHIR® Release 4, the applicable implementation guide would be US Core STU 3.1.0, which is expected to be published late 2019.

We also support ONC's establishment of the proposed initial set of FHIR® resources to be used for the proposed APIs, the "API Resource Collection in Health" (ARCH), which would align with the proposed USCDI. Although we believe that, in general, health IT standards should be developed by standards developing organizations (SDOs), we recognize the considerations that lead ONC to publish the ARCH. We ask ONC to specify that the ARCH is bounded by the scope of the USCDI, that the USCDI will only include data classes and data elements that have SDO-

[3] https://www.healthit.gov/isa/data-segmentation-sensitive-information

developed implementation guides, that the ARCH will only reference HL7® FHIR® resources, and, moving forward, that the function of the ARCH is transitioned as rapidly as possible to a private sector, SDO-developed implementation specification, such as the HL7® US Core.

B.5. Real World Testing

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. In this proposed rule, ONC outlines what successful "real world testing" means for the purpose of this Condition of Certification, as well as proposed Maintenance requirements—including standards updates for widespread and continued interoperability.

Comment: We strongly support the requirement for real-world testing as required by the Cures Act and generally as proposed by ONC. We agree with ONC that required testing should be limited to health IT developers with Health IT modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange.

We also support the Standards Version Advancement Process (SVAP) as supporting innovation and enabling needed industry flexibility. We view the ONC certification program as providing a floor that all certified technology will need to support, while the SVAP provides permissible progressions (that later can become the new floor in a future rule). To maintain compatibility, support for this floor is critical to avoid adoption of only the SVAP allowed version and not being able to fully communicate with the floor version. With respect to the SVAP's ability to assert conformance in the absence of the test tools, there is a need to test once those tools do become available.

We strongly support ONC's proposal that "developers should consider existing testing tools and approaches that may be used to assess real world interoperability. For example, we encourage health IT developers to consider metrics of use and exchange from existing networks, communities, and tools including, but not limited to, Surescripts, Carequality, CommonWell Health Alliance, the C–CDA One-Click Scorecard, and DirectTrust."

D. Enforcement

ONC proposes a general enforcement approach to encourage consistent compliance with the requirements.

Comment: In general, we agree with the enforcement approach taken for the conditions of certification and the relative roles of ONC and the ONC-ACBs, including building on processes previously established for ONC direct review of certified health IT. We strongly agree with ONC's proposed approach to focus on a corrective action process as the first priority in its enforcement engagement with developers. We also emphasize the need for clarity on the interaction of enforcement for these provisions as reflected in Table 3 (p. 7507) and for information blocking more generally as well as the relative roles of the OIG and ONC. We appreciate the discussion of

OIG and ONC roles on p. 7507 and emphasize the critical need for both clarity and coordination in roles.

V.III. Information Blocking

Section 4004 of the Cures Act establishes stringent requirements around the prohibition of information blocking. The statutory language adds some clarity but also requires ONC to define key terms and concepts in this regulation as well as to identify "reasonable and necessary [activities that interfere with the access, exchange, or use of EHI and] that do not constitute information blocking". ONC also proposes a complaint and enforcement process that could, but need not, coordinate with the OIG and Federal Trade Commission and that would supersede certification bodies in some cases.

Comment: Although much of the focus of the proposed rule is on the Secretary's identification of "reasonable and necessary [activities that interfere with the access, exchange, or use of EHI and] that do not constitute information blocking," we emphasize that ONC's regulatory actions in proposed definitions, as well as its regulatory and sub-regulatory discussions and provisions regarding information blocking and definitions, are also of great importance. In the sections below, we provide our focused comments. In addition, we commend to ONC the comments of the Sequoia Project on this issue as well as the work of the Information Blocking Workgroup of Sequoia's Interoperability Matters Cooperative, attached as Appendix 2 to these comments.

C. Relevant Statutory Terms and Provisions (p. 7509)

Comment: ONC defines several terms used in the Cures Act. Although we do not have specific suggestions for changes for most of these terms, we emphasize that the definitions of "access," "exchange," "use," and "electronic health information" (EHI) are very broad. As they interact with each other, with the definitions of the four types of actors, with the ONC descriptions and examples of information blocking practices, and with the seven exceptions, the result is an extensive and diverse set of scenarios and use cases that will be subject to complex compliance and enforcement processes. We are concerned that the impact, foreseen and unforeseen, may exceed and even be inconsistent with Congress' intent to define and limit information blocking.

We are especially concerned with the implications of the very broad definition of EHI and the likely impracticality of applying the information blocking provisions to this extensive, highly situational and largely non-standardized data set. We suggest that enforcement be primarily focused on supporting access to and exchange and use of the USCDI (including API access), which will evolve over time to include more and more EHI, including data elements to support payer-relevant data elements to support CMS and other payer priorities. We pledge to work closely with the community and ONC to achieve this goal.

Of great concern are the definitions of "Health Information Exchanges" (HIEs) and "Health Information Networks" (HINs). We believe that the distinctions between these two categories are unclear. More generally, these definitions should align with congressional intent as well as common industry understanding of what these terms mean.

Getting these definitions right is critical for several reasons, including the prospect of sweeping in organizations (e.g., provider organizations) that would otherwise not have liability for the very

high maximum fines applicable to HIEs and HINs that engage in information blocking. These definitions would also subject a broad array of organizations to the very stringent requirements associated with these exceptions, for example, permissible contracting practices and terms, down-time for maintenance, and establishment of fees.

For HINs, we believe that the definition is too broadly defined and does not accord with the commonly accepted definition of a network. ONC states that:

> *Health Information Network or HIN means an individual or entity that satisfies one or both of the following—*
>
> *(1) 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 electronic health information between or among two or more unaffiliated individuals or entities*
>
> *(2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.*

The examples of HINs in the preamble go well beyond the reasonable definition of a "network," a term that is not defined in the proposed rule. ONC provides as examples of an HIN:

- *Entity established in a state to improve movement of EHI between providers operating in state; identifies standards for security and offers terms and conditions for providers wishing to participate in the network.*
- *Entity offering (and overseeing and administering) terms and conditions for network participation.*
- *Health system administers agreements to facilitate exchange of EHI for use by unaffiliated family practices and specialist clinicians to streamline referrals.*
- *Individual or entity that does not directly enable, facilitate, or control movement of information, but exercises control or substantial influence over policies, technology, or services of a network.*
- *A large provider may decide to lead an effort to establish a network that facilitates movement of EHI between group of smaller providers (and the large provider) and through technology of health IT developers; large provider, with some participants, creates a new entity that administers network's policies and technology*

We especially note the fourth example, which follows from the first part of the definition and focuses on policies. We strongly encourage ONC to revise the definition of a HIN for this rule to be (a) be an actual network or a formalized component of an actual network and (b) have an actual operational role and responsibility for the network. Organizations that develop voluntary standards and policies that may be used by one or more HINs (e.g. standards development organizations—SDOs), should not be considered HINs. Nor should organizations that provide administrative or operational support for an HIN but that do not have governance responsibility or operational control. We also believe ONC should not define hospitals or other healthcare organizations with limited exchange capabilities (e.g., interfaces for ADT messages or lab results) as an HIN for the purpose of these regulations.

We also ask ONC to clarify the extent of the responsibility of a network with respect to its constituent organizations and their own policies and actions that may implicate information blocking. For example, if an HIN knows or should have known that a member engaged in practices that could implicate information blocking, what is the HIN's responsibility to apply the exceptions and other considerations to determine whether a violation occurs, or is the HIN only responsible for its own actions? We believe that the latter should be the case. In addition, to what extent must a HIN ensure that its policies specifically prohibit information blocking by its members or is it enough to ensure that its policies do not require or encourage information blocking?

Finally, we tend to see HIEs as an organizational type (versus the use of "HIE" as a verb) and as a subset of HINs. We do not have significant concerns with the proposed definition of an HIE other than that, as indicated, we believe that the distinctions between HIEs and HINs are unclear. For example, ONC states that an HIE that facilitates access, exchange, or use for more than a narrowly defined set of purposes, may be an HIE and an HIN. Given that the information blocking definitions and penalties are the same for both HINs and HIEs, we suggest that ONC consider combining these in a single category—"HIE and HIN".

c. Examples of Practices Likely to Interfere with Access, Exchange, or Use of EHI (p. 7518)

ONC provides examples of practices that may implicate information blocking, indicating that these practices can be mitigated by application of one or more of the "reasonable and necessary" exceptions included in the proposed rule. (Quoted language below comes from this section.)

Comment: We find these examples helpful and they should provide a useful basis for sub-regulatory guidance that can assist the industry in achieving more cost-effective compliance. At the same time, some of the examples raise issues that point to potential needs for revisions in both ONC regulatory provisions and agency interpretations.

i. Restrictions on Access, Exchange, or Use

"One means by which actors may restrict access, exchange, or use of EHI is through formal restrictions. These may be expressed in contract or license terms, EHI sharing policies, organizational policies or procedures, or other instruments or documents that set forth requirements related to EHI or health IT."

- "A HIN's participation agreement prohibits entities that receive EHI through the HIN from transmitting that EHI to entities who are not participants of the HIN."

Comment: We are concerned that this example could be interpreted as preventing an HIN from restricting participation in the HIN to those who have signed its participation agreement and agreed to abide by reasonable and necessary policies. The distinction between such an action, and the action of preventing, by policy, information from being shared with non-participants through means unrelated to the HIN, should be clarified.

We also ask ONC to be clear that an HIN can restrict exchange within the HIN to entities that sign the HIN's participation agreement. More generally, we believe that HINs should be expected to connect with other HINs for applicable use cases through a network-to-network trust agreement or

the TEFCA. In addition, an HIN should be able to require that EHI received through the HIN be protected in a manner consistent with state and federal law.

"Access, exchange, or use of EHI can also be restricted in less formal ways. The information blocking provision would be implicated, for example, where an actor simply refuses to exchange or to facilitate the access or use of EHI, either as a general practice or in isolated instances. The refusal may be expressly stated, or it may be implied from the actor's conduct, as where the actor ignores requests to share EHI or provide interoperability elements; gives implausible reasons for not doing so; or insists on terms or conditions that are so objectively unreasonable that they amount to a refusal to provide access, exchange, or use of the EHI"

Comment: An HIN or HIE should be able to choose not to exchange data with another party that has not agreed to the terms of a reasonable governance and trust framework. We recognize that a given policy that is consistent with the information blocking provisions may not be the only way to achieve compliant exchange, but it should be acceptable to limit exchange to parties that agree to a reasonably developed, compliant framework.

iv. Rent-seeking and Other Opportunistic Pricing Practices

"Certain practices that artificially increase the cost and expense associated with accessing, exchanging, and using EHI will implicate the information blocking provision. Such practices are plainly contrary to the information blocking provision and the concerns that motivated its enactment . . . An actor may seek to extract profits or capture revenue streams that would be unobtainable without control of a technology or other interoperability elements that are necessary to enable or facilitate access, exchange, or use of EHI".

Comment: In general, we are very concerned with the complexity and broad reach resulting from the interaction of the pricing provisions of the proposed rule for information blocking practices and exceptions, with the very expansive definitions of actors and of EHI. Although the heading of this section refers to "rent-seeking and other opportunistic pricing practices," ONC is clear in the proposed rule preamble that its definition of the types of fees that could implicate as information blocking is not limited to such behaviors, whose identification is likely to be very subjective. For example, ONC implies that "value-based pricing," an approach commonly used in industry and indeed one increasingly used in healthcare to pay for drugs and health plans is "opportunistic" and would not be mitigated by any of the proposed exceptions. ONC goes on to emphasize that

- "[T]he reach of the information blocking provision is not limited to these types of practices. We interpret the definition of information blocking to encompass any fee that materially discourages or otherwise imposes a material impediment to access, exchange, or use of EHI. We use the term "fee" in the broadest possible sense to refer to any present or future obligation to pay money or provide any other thing of value . . . We believe this scope may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services. Therefore, . . . we propose to create an exception that, subject to certain conditions, would permit the recovery of costs that are reasonably incurred to provide access, exchange, and use of EHI."

It appears that ONC would view any fee as imposing a "material impediment" and therefore requiring use of the exception focused on recovering costs. ONC acknowledges that the definition of <u>any</u> fee as a practice that implicates information blocking "may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services". We agree with ONC on this latter point but are not convinced that simply providing an exception, which is itself very limiting, is a sufficient counter to the issues raised by the provision. In addition, the documentation required by these exceptions could be quite extensive and onerous.

Certainly, where fees are established by market-based business models, especially for actors that are not actually networks or HIEs as these terms are commonly understood, it seems undesirable that these organizations would be subject to the detailed fee regulation established through the combination of the practice and the exception. For example, we do not believe that a mutually agreeable decision to share in revenue should be prohibited for every actor for any interoperability element. We suggest that there be a narrower definition and associated interpretation of HIE and especially HIN, and that more flexibility be provided for revenue-sharing arrangements that do not introduce unreasonable or unnecessary costs but rather may enable provision of valuable products and services.

<u>v. Non-Standard Implementation Practices</u>

"Even where no standards exist for a particular purpose, actors should not design or implement health IT in non-standard ways that unnecessarily increase the costs, complexity, and other burden of accessing, exchanging, or using EHI."

- An EHR developer of certified health IT implements the C-CDA® for receiving transitions of care summaries but only sends transitions of care summaries in a proprietary or outmoded format.
- A health IT developer of certified health IT adheres to the "required" portions of a widely adopted industry standard but chooses to implement proprietary approaches for "optional" parts of the standard when other interoperable means are readily available.

Comment: We agree with the importance of standardized implementations; achieving such standardization, including further standardization of SDO implementation specifications, has been essential to the success of large-scale health data sharing initiatives to date, especially Carequality.

At the same time, certain types of optionality, especially for specialized use cases, can be very important to support innovation and specific use cases. For example, specialized data fields that lack a widely accepted terminology standard may need to be collected and shared to accommodate specialty workflows, such as multidisciplinary tumor boards in oncology. Actors could reasonably develop and enforce a new terminology standard for these specialized fields that, by definition, will not be widely adopted initially, without implicating information blocking. Their behavior would cross the line into information blocking, however, if they insist that the specialized data be transmitted in a way that is not aligned with widely adopted communications formats, for example, where both FHIR® and CDA® could accommodate the

information. Careful and flexible application of this information blocking practice will be essential given the complexities of health IT implementation.

6. Applicability of Exceptions
a. Reasonable and Necessary Activities (p. 7522)

ONC describes three overarching policy considerations that guided development of these seven exceptions. First, the exceptions would be limited to certain activities that clearly advance the aims of the information blocking provision; promoting public confidence in health IT infrastructure by supporting the privacy and security of EHI and protecting patient safety; and promoting competition and innovation in health IT and its use to provide health care services to consumers. Second, each exception is intended to address a significant risk that regulated individuals and entities will not engage in these reasonable and necessary activities because of *potential uncertainty* regarding whether they would be considered information blocking. Third, and last, each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt. To qualify for any of these exceptions, an individual or entity would, for each relevant practice and at all relevant times, must satisfy *all* applicable conditions of the exception.

Comment: These are appropriate policy considerations. Overall, we believe that the seven categories of exceptions are the right ones and indeed, are essential to implementation of the information blocking prohibition. We do have overall concerns as well as questions about specific elements. We especially highlight our concern with the proposed requirement that "[t]o qualify for any of these exceptions, an individual or entity would, for each relevant practice and at all relevant times, must satisfy all applicable conditions of the exception". Such a strict compliance standard may add clarity, but it is at odds with the complexity that underlies healthcare operations. We also have general concerns with the costs and complexity that will be the result of organizations needing to manage these complex policies and to document their actions and associated rationale.

Below, we comment selectively on the proposed exceptions. More generally, we suggest that ONC consider the comments and recommendations on the exceptions included in report of the Information Blocking Workgroup of the Interoperability Matters Cooperative, included as Appendix 2 to these comments on this proposed rule.

1. Preventing Harm—§171.201

Comment: We have a few specific points to make:

- *We are concerned that ONC's expectations for the ability to carve out 42 CFR Part 2 covered data may far exceed current industry capabilities in terms of technology and operational capacity. In particular, carving out such data from clinical notes for exchange and data export will be very challenging.*

- *We suggest that the focus on physical harm in the determination by a licensed health care professional that disclosure of EHI is reasonably likely to endanger the life or physical safety of a patient or another person is too narrow and should be expanded to include psychological and other forms of non-physical harm.*

2. Promoting the Privacy of EHI—§171.202

Comment: For 202(b)(2)(i), we are concerned that the requirement that the actor "[d]id all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization" is too rigid a requirement. If even one possible action was not done, the exception would not apply. Moreover, for an HIN that does not have operational control over or visibility into the detailed decision-making of its participants, it would not be possible to apply or validate this test. We ask ONC to explicitly indicate that an actor such as an HIN does not have the obligation to review or confirm that the actions of its participants meet this or other exception tests that do not involve direct decisions by the HIN. A key issue for a trust framework like Carequality, and likely any nationwide HIN, is that the terms of a trust agreement, may (out of necessity) provide reasonable discretion for the network participants. One such example is enabling participants to accommodate variations in privacy laws across states as necessary. Doing so could also be potentially construed as enabling decisions that implicate information blocking. It is essential, therefore that ONC focus on direct HIN decisions rather than the actions of its participants, which may or may not have been enabled by the HIN's trust agreement.

3. Promoting the Security of EHI—§171.203

Comment:

- *We ask that ONC confirm that an HIN or HIE requiring the use of digital certificates that meet federal agency standards in order to meet the needs of its participants will be consistent with this exception when it imposes such requirements.*

- *In addition, we offer the scenario of an organization that launches an IHE XCPD query that is otherwise compliant with an HIN's specifications but is rejected because the query is not secured with an HIN certificate. We ask that ONC clarify that such a request for data access can be rejected, without violating this exception, as not compliant with an organization's reasonably adopted privacy and security policies, including those involving certificates, and the need to validate the identity of the requester and the requester's valid right to access the data.*

- *ONC should address the extent to which actions by an actor to address legal liability not mitigated by HHS Office of Civil Right (OCR) HIPAA-related policies can support use of this exception, including potential liability that can come with exchange that is not covered by OCR guidance relating to the HIPAA patient right of access. Such liability could arise from such sources as state laws, FTC regulations, or contractual obligations.*

- *We ask the Department to ensure that the HHS Office of Civil Rights (OCR) issues guidance that conforms, as necessary, to final ONC information blocking regulations.*

- *We are concerned with a lack of standards and definitions of such terms as "directly related" and "tailored" and the burden on the industry (including providers, developers, HIEs and HINs) to perform analyses of their policies and practices against such complex and incompletely defined terms and tests, especially with the requirement to meet "all*

requirements at all times".

- *We note that this exception has a provision for cases where there is no written policy (171.203(e)). In practice, it seems most likely that the absence of a policy means that one is dealing with an unexpected and evolving situation as best one can (e.g., a sustained and sophisticated attack). The exception calls for not only a determination that the practice is necessary, but that effectively there is no other way of having protected your security that might have been less likely to interfere with information access. In our view, such a requirement is asking too much of those dealing with urgent threats, often after hours and under considerable uncertainty. We suggest that 171.203(e)(2) have a further "safety valve" for short-lived actions that are taken in good faith while a situation is being evaluated and understood.*

- *We ask that ONC clarify that proactive and preventive security-focused activities that are a condition of exchange are permitted, so long as they meet the applicable criteria for security-related practices in this exception.*

4. Recovering Costs Reasonably Incurred—§171-204.

   Comment:

   - *We do not believe that all mutually agreeable decisions to share in revenue should be prohibited for every actor for any interoperability element.*

   - *We are concerned that requirements for very granular costs and fee accounting will significantly increase the cost of doing business and of data exchange. We are concerned that the exception can be read to require that an actor retain extensive records to document all of the costs that the actor incurred to develop an interoperability element so that it can prove that its fees only recover those costs plus a "reasonable" profit. Cost accounting is challenging for even very large and well-resourced organizations and we are concerned that this exception will result in unintended negative consequences for many actors. We request that ONC clarify that this outcome is not the intent of this exception and to take steps to mitigate the risks of such an outcome.*

   - *We ask that ONC recognize that for many organizations, especially non-profits, it is common and appropriate for fees to scale with the size of a member/participant organization. We suggest that such an approach, which does not focus on the revenue or profits for exchange that is facilitated by the organization establishing the fees, is appropriate and that basing fees on member size is a reasonable proxy for basing fees in relation to current costs as well as the need to invest in future capabilities. Such organizations would, in general, be able to demonstrate that aggregate fees collected are related to and grounded in costs but not that a specific fee is directly related to specific costs.*

   - *We ask ONC to state that it is not information blocking when an organization (e.g., an HIE or HIN) has a policy that its participants cannot condition their provision of information on the recipient paying a fee for certain use cases or permitted purposes,*

such as treatment (i.e., an HIE or HIN would be permitted to prohibit charging certain types of fees under specific circumstances without that policy implicating information blocking).

- *We agree that ONC should prioritize exchange, access, and use of "observational health information" (i.e., EHI that is created or maintained during the practice of medicine or the delivery of health care services to patients). In addition, we believe that ONC should also prioritize certain purposes or use cases for data exchange/access/use, specifically, the HIPAA categories of treatment, payment, and operations, relative to access (other than that needed to support a patient's HIPAA right of access) intended to serve primarily commercial objectives of the party seeking data.*

- *We ask ONC to clarify if the fees established by an IT vendor supporting an HIE or an HIN are subject to this provision and if an HIE or HIN implicates information blocking if it passes on third-party fees as a cost when it has no direct control over such fees? In this scenario, we do not think that the actions of the HIE or HIN should implicate information blocking and that their fees should be able to meet this exception.*

5. Responding to Requests for Access, Exchange, and Use that are Infeasible—§171-205

   Comment:

   - *Requests for data that would require the use of non-standard implementation specifications should be able to be refused as "infeasible"*

   - *Actors should be able to focus on specific use cases and refuse requests to expand access, exchange, or use to support additional use cases as "infeasible." At the same time, we believe that there should be a floor defining the minimum set of use cases with associated interoperability standards that must be supported by a specific type of actor; perhaps the TEFCA provides a basis for such a floor.*

   - *Requests to participants of an HIE or HIN that maintains a trust agreement/framework should be able to be refused if the requester does not participate in the applicable trust framework or act consistently with its provisions, even if the HIE or HIN has a dominant market position, so long as the terms of the trust agreement are not discriminatory or deliberately anti-competitive.*

In addition, ONC asks if it should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices necessary to comply with the requirements of the Common Agreement (TEFCA).

Comment: We believe that such an exception should be created and suggest that ONC broaden this exception to include compliance with the terms of private sector trust frameworks whose aim is to enhance interoperability. We urge that ONC explicitly indicate that such trusted exchange frameworks can design and implement agreements that impose specific obligations on participants, and also that they can employ specific provisions intended to gain participation and hence, to enable greater flow of EHI. We also ask ONC to be clear that such frameworks can

choose, and HINs more generally can choose, to focus on specific EHI-exchange use cases and not to address others, potentially subject to a minimum floor as discussed above.

Patient Matching Request for Information (p. 7554)

General Comments: In our detailed comments below, we address the questions that ONC poses in its request for information (RFI) and agree with ONC on the importance of this issue and of the role of the private sector, with federal government support, in improving patient match rates. We point ONC to the Sequoia Project's "A Framework for Cross-Organizational Patient Identity Management," first published in 2016 and updated in 2018.[4] We especially emphasize that much of the focus in accurate patient matching has been intra-organizational but that true interoperability and data liquidity will require accurate cross-organizational matching.

More generally, although federal agencies are restricted to patient matching approaches instead of use of a unique identifier, the private sector should not be subjected to that restriction. We urge ONC to support and enable a competitive marketplace for secure identity solutions from commercial third-party enterprises. In addition, it is important to note that identity requirements for Payment and health care Operations are fundamentally different than identity requirements for Treatment. Financial transactions are reversible, and reports can be corrected, but patient care actions are often permanent. Accordingly, in our experience, providers have lower tolerance for false positives, and the different purposes of use should not be subjected to a lowest common denominator patient matching approach.

ONC asks several questions in this RFI, and we address several of these below.

1. It is a common misconception that technology alone can solve the problem of poor data quality, but even the most advanced, innovative technical approaches are unable to overcome data quality issues. Thus, we seek input on the potential effect that data collection standards may have on the quality of health data that is captured and stored and the impact that such standards may have on accurate patient matching. We also seek input on other 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 elements such as mailing address, as well as other efforts that support ongoing data quality improvement efforts.

   Comment: We agree with ONC that data collection standards and their consistent application by providers and exchange organizations are a critical determinant to matching accuracy. The above-referenced Sequoia Project document addresses this issue in detail, including, notably, a maturity model for intra-organizational and cross-organizational processes to enhance patient matching accuracy, including rigorous information governance. Overall, the biggest opportunity to immediately enhance matching rates is standardized formats for demographic data among data sharing participants.

[4] https://sequoiaproject.org/resources/patient-matching/

2. In concert with the GAO study referenced above, we seek input on what additional data elements could be defined to assist in patient matching as well as input on a required minimum set of elements that need to be collected and exchanged. We encourage stakeholders to review the Patient Demographic Record Matching section of the Interoperability Standards Advisory (ISA) and comment on the standards and implementation specifications outlined.

   Comment: Additional data elements to improve patient matching efforts may include: Maiden Name, Multiple Birth Indicator, Birth Order, Telephone Number types, and Email Address(es). In addition, substantially increased patient match rates (i.e., above 95%) may require a supplemental identifier in addition to the required fields. A supplemental identifier could be a national or regional shared identifier, such as a driver's license number. High data quality of any such identifier at the point of capture is essential for acceptable patient match rates.

3. Also, in alignment with the GAO study, we seek input on whether and what requirements for electronic health records could be established to assure data used for patient matching is collected accurately and completely for every patient. For instance, the adopted 2015 Edition "transitions of care" certification criterion (§ 170.315(b)(1)) currently includes patient matching requirements for first name, last name, previous name, middle name, suffix, date of birth, address, phone number, and sex. These requirements also include format constraints for some of the data.

   Comment: As discussed above, other potential data elements of value include: Maiden Name, Multiple Birth Indicator, Birth Order, Telephone Number types (we note the high value of the validated cell phone number), and Email Address(es). We also highlight the importance of consistently defined and enforced format constraints.

4. There are unique matching issues related to pediatrics and we seek comment on innovative and effective technical or non-technical approaches that could support accurate pediatric record matching.

   Comment: We agree there are special challenges for pediatric populations, with matching for newborns being especially problematic. Issues unique to pediatrics include

   - *No national naming convention for newborns, specifically, patients who have not yet received their legal name and have a temporary name; and*
   - *Multiple births present challenges with same date of birth, address, mother's maiden name and potentially very similar names and identifiers, often only differing by a single digit.*

Specific approaches to enhance patient matching accuracy for pediatrics include:

- *Following the Children's Hospital Association's temporary demographic conventions for newborns;*
- *Standards adoption (e.g., for naming, demographics and gender identification);*
- *Information governance, process, and technology (e.g., ensuring the health IT and its use enables complete and accurate medical records both for the mother and fetus);*
- *Vendor capture of multiple birth indicator, birth order, and mother's maiden name; and*
- *Creation of the medical record prior to birth event*

5. Recent research suggests that involving patients in patient matching may be a viable and effective solution to increase the accuracy of matching, and giving patients access to their own clinical information empowers engagements and improved health outcomes. We seek comment on potential solutions that include patients through a variety of methods and technical platforms in the capture, update and maintenance of their own demographic and health data, including privacy criteria and the role of providers as educators and advocates.

   Comment: We believe that involving the patient in data entry, correction, and maintenance can maintain and enhance patient data integrity over time. This approach includes making it a practice to ask the patient at every visit (and training staff on the value of doing so) whether their address or other contact information has changed and also having the patient review their demographic data to ensure its correctness. Patient portals and other self-service applications can also help patients understand the extent of their identity data completeness and how it can be increased.

   More generally, we emphasize that more complete demographic data will only get us so far. We believe that healthcare should increasingly look to approaches like biometric data, that rely on data that is "patient inherent" rather than simply "patient-verified".

7. At the same time, we seek input on transparent patient matching indicators such as database duplicate rate, duplicate creation rate, and true match rate, for example, that are necessary for assessment and reporting. The current lack of consensus, adoption, and transparency of such indicators makes communication, reporting, and cross-provider or cross-organizational comparisons impossible, impedes a full and accurate assessment of the extent of the problem, prohibits informed decision making, limits research on complementary matching methods, and inhibits progress and innovation in this area.

   Comment: We agree on the value of such transparent indicators, but emphasize that a gold standard, curated data set with known "correct answers" relative to matching is necessary to effectively evaluate algorithms.

8. There are several emerging private sector led approaches in patient matching that may prove to be effective, and we seek input on these approaches, in general. A number of matching services that leverage referential matching technology have emerged in the market recently, yet evaluations of this type of approach has either not been conducted or has not been made public. Other innovative technical approaches such as biometrics, machine learning and artificial intelligence, or locally developed unique identifier efforts, when used in combination with non-technical approaches such as patient engagement, supportive policies, data governance, and ongoing data quality improvement efforts may enhance capacity for matching.

   Comment: In the future, biometrics will likely play a very significant role in patient matching and identity proofing and may change the fundamental paradigm for patient identification. Examples of biometrics include fingerprint, palm veins, facial recognition, DNA, palm print, hand geometry, iris recognition, and retinal scanning. Biometric devices are used to capture these metrics in a systematic and reliable way. Biometrics are considered immutable attributes, in that they are innate, entrenched, and would take significant effort to change. As such, biometric attributes are ideal for patient matching and identity proofing and we encourage ONC to facilitate and identify standards in this area that can encourage interoperability of biometric data.

9. Finally, ONC seeks input on new data that could be added to the United States Core Data for Interoperability (USCDI) or further constrained within it in order to support patient matching.

   Comment: Additional data elements for consideration include: Maiden Name, Multiple Birth Indicator, Birth Order, Telephone Number types, and Email Address(es) and types.

Appendix 2: Recommendations of the Information Blocking Workgroup of the Interoperability Matters Forum

Information Blocking Workgroup

Final Report on ONC March 2019 Proposed Rule: Information Blocking Provisions

Interoperability Matters

4/30/2019

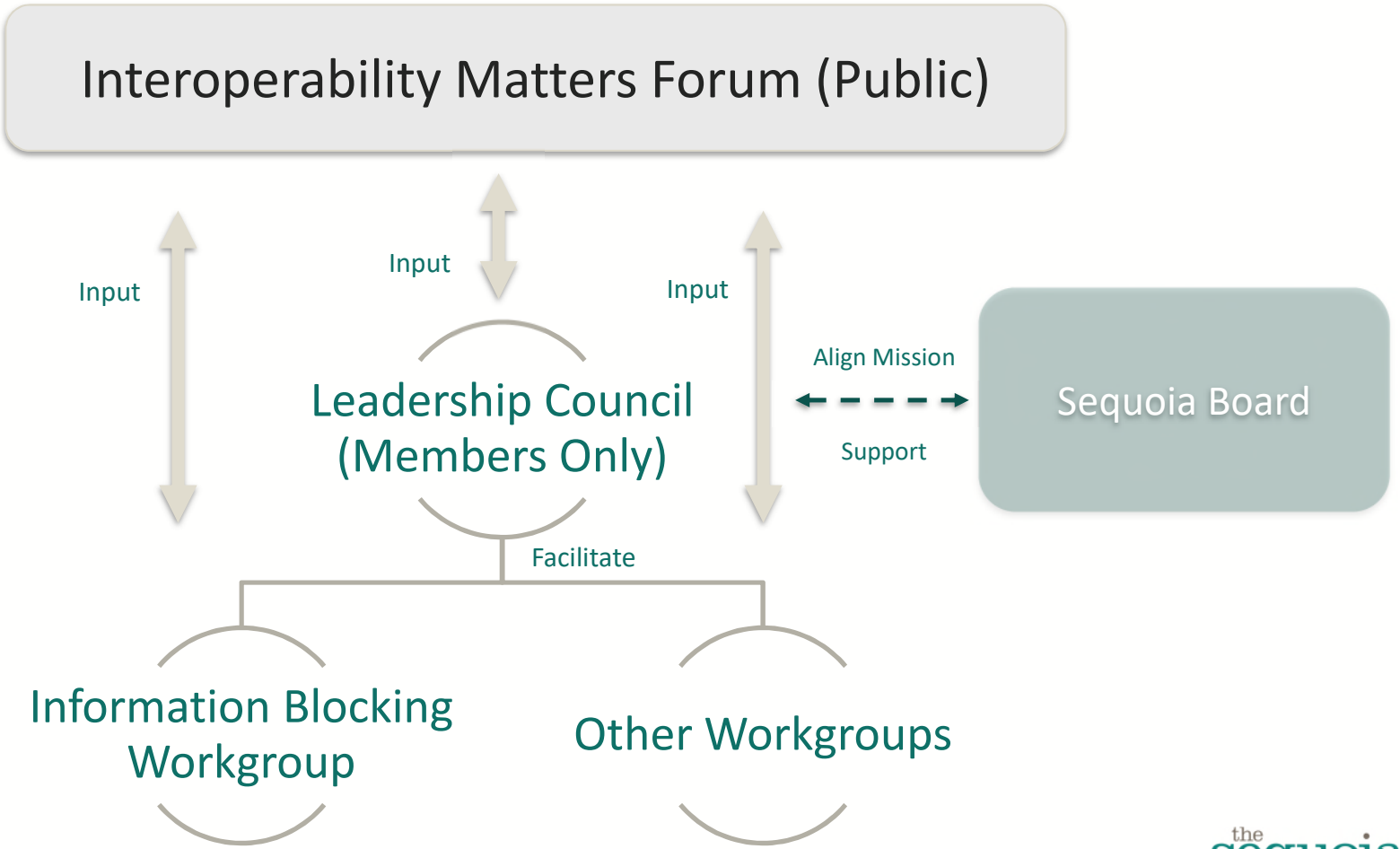
Organization of the Report

- Background on the Workgroup
- Findings
  - Actors and Other Definition
  - Information Blocking Practices
  - Exceptions
    - Preventing Harm
    - Privacy
    - Security
    - Recovering costs reasonably incurred
    - Declining to provide access, exchange, or use of EHI if request is infeasible
    - Licensing technologies or other interoperability elements
    - Making health IT unavailable to perform maintenance or improvements
  - Request for Information: Disincentives for Providers
- Next Steps

Interoperability Matters Cooperative: Function

- Prioritize matters that benefit from national-level, public-private collaboration
- Focus on solving targeted, high impact interoperability issues
- Engage the broadest group of stakeholders and collaborators
- Coordinate efforts into cohesive set of strategic interoperability directions
- Channel end user needs and priorities
- Bring forward diverse opinions, which may or may not result in consensus
- Facilitate input and develop work products, with implementation focus
- Support public forum for maximum transparency
- Provide feedback based upon real world implementation to policy makers
- Deliver work products and implementation resources

Interoperability Matters: Structure



Interoperability Matters Advisory Forum (Public)

- Provides open, public forum to provide input and assure transparency
- Serves as listening session for staff, workgroup and Leadership Council
- Represents diverse private / public stakeholder and end user perspectives
- Provides input into the priorities and work products
- Enables community to share tools, resources and best practices
- Provides venue for policy makers to hear diverse perspectives in real-time

Information Blocking Workgroup: Purpose

- Identify practical, implementation-level implications of proposed and final information blocking rules, which may or may not be consensus positions
- Provide input into Sequoia comments to ONC on proposed rule
- Facilitate ongoing discussions to clarify information blocking policies and considerations prior to and after the Final Rule

Information Blocking Workgroup: Scope and Focus of Review

- Primary: *Information Blocking* part of ONC proposed rule
  - Definitions (including Information Blocking Practices and Actors)
    - Identify implications and suggest revisions
  - Information blocking practices with examples
    - Add, revise, delete
  - Reasonable and Necessary Exceptions
    - Add, revise, delete
    - Activities that are info blocking, but are reasonable and necessary according to ONC criteria
  - Specific ONC comments sought
  - ONC RFI: disincentives for providers and price transparency
  - Complaint process and enforcement
- Secondary:
  - Information Blocking elements of Conditions and Maintenance of Certification, including enforcement

Workgroup Representatives

Associations and Orgs - health IT community
- Mari Greenberger, HIMSS
- Matt Reid, AMA
- Lauren Riplinger, AHIMA
- Scott Stuewe, DirectTrust

Consumers
- Ryan Howells, CARIN Alliance
- Deven McGraw, Ciitizen

Federal Government
- Steve Bounds, SSA
- Margaret Donahue, VA

Health Information Networks and Service Providers
- Angie Bass, Missouri Health Connect
- Dave Cassel, Carequality
- Laura Danielson, Indiana Health Information Exchange
- Paul Uhrig, Surescripts, Co-Chair

Healthcare Provider
- David Camitta, Dignity, Co-Chair
- Eric Liederman, Kaiser Permanente

Legal, Technology, Standards, and Policy Subject Matter Experts
- Jodi Daniel, Crowell & Moring, LLP
- Josh Mandel, Microsoft
- Micky Tripathi, MaEHC

Payers
- Nancy Beavin, Humana
- Danielle Lloyd, AHIP
- Matthew Schuller, BCBSA

Public Health
- John Loonsk, APHL

Vendors
- Brian Ahier, Medicity / Health Catalyst
- Aashima Gupta, Google
- Cherie Holmes-Henry, EHRA / NEXTGEN
- Rob Klootwyk, Epic
- Josh Mast, Cerner

Informatics
- Doug Fridsma, AMIA

Safety net providers / service provider
- Jennifer Stoll, OCHIN

Release of Information Company
- Rita Bowen, MROCorp

The Sequoia Project Team

Lindsay Austin, Troutman Sanders Strategies

Didi Davis, VP, Informatics, Conformance & Interoperability

Steve Gravely, Gravely Group - Facilitator

Shawna Hembree, Program Manager

Mark Segal, Digital Health Policy Advisors - Facilitator

Dawn VanDyke, Director, Marketing Communications

Mariann Yeager, CEO

Deliverables

- Perspectives on ONC 21st Century Cures proposed rule that inform industry and Sequoia Project regulatory comments
- Assessments of proposed rule implications to the community
- Assessments of ONC proposed rule, with identified follow-up actions needed by federal government and private sector

7424 Federal Register / Vol. 84, No. 42 / Monday, March 4, 2019 / Proposed Rules

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 170 and 171

RIN 0955–AA01

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

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Proposed rule.

SUMMARY: This proposed rule would implement certain provisions of the 21st Century Cures Act, including conditions and maintenance of certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program), the voluntary certification of health IT for use by pediatric health care providers, and reasonable and necessary activities that do not constitute information blocking. The implementation of these provisions would advance interoperability and support the access, exchange, and use of electronic health information. The proposed rule would also modify the 2015 Edition health IT certification criteria and Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

DATES: To be assured consideration, written or electronic comments must be received at one of the addresses provided below, no later than 5 p.m. on May 3, 2019.

ADDRESSES: You may submit comments, identified by RIN 0955–AA01, by any of the following methods (please do not submit duplicate comments). Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

• *Federal eRulemaking Portal:* Follow the instructions for submitting comments. Attachments should be in Microsoft Word, Microsoft Excel, or Adobe PDF; however, we prefer Microsoft Word. *http://www.regulations.gov.*

• *Regular, Express, or Overnight Mail:* Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Attention: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201. Please submit one original and two copies.

• *Hand Delivery or Courier:* Office of the National Coordinator for Health Information Technology, Attention: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201. Please submit one original and two copies. (Because access to the interior of the Mary E. Switzer Building is not readily available to persons without federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Enhancing the Public Comment Experience: To facilitate public comment on this proposed rule, a copy will be made available in Microsoft Word format on ONC's website (*http://www.healthit.gov*). We believe this version will make it easier for commenters to access and copy portions of the proposed rule for use in their individual comments. Additionally, a separate document ("public comment template") will also be made available on ONC's website (*http://www.healthit.gov*) for the public to use in providing comments on the proposed rule. This document is meant to provide the public with a simple and organized way to submit comments on proposals and respond to specific questions posed in the preamble of the proposed rule. While use of this document is entirely voluntary, we encourage commenters to consider using the document in lieu of unstructured comments, or to use it as an addendum to narrative cover pages. We believe that use of the document may facilitate our review and understanding of the comments received. The public comment template will be available shortly after the proposed rule publishes in the **Federal Register**. This short delay will permit the appropriate citation in the public comment template to pages of the published version of the proposed rule.

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. Please do not include anything in your comment submission that you do not wish to share with the general public. Such information includes, but is not limited to: A person's social security number; date of birth; driver's license number; state identification number or foreign country equivalent; passport number; financial account number; credit or debit card number; any personal health information; or any business information that could be considered proprietary. We will post all comments that are received before the close of the comment period at *http://www.regulations.gov.*

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201 (call ahead to the contact listed below to arrange for inspection).

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

Table of Contents

Key Concepts for Workgroup Review

Actors

- Health Care *Providers*
- *Developers* of Certified Health IT
- Health Information *Exchanges*
- Health Information *Networks*

Blocking Practices

- *Restrictions on access, exchange, or use* of EHI through formal means (e.g., contractual restrictions) or informal means (e.g., ignoring requests to share EHI)
- *Limiting or restricting the interoperability of health IT* (e.g., disabling a capability that allows users to share EHI with users of other systems)
- *Impeding innovations and advancements* in access, exchange, or use or health IT-enabled care delivery (e.g., refusing to license interoperability elements to others who require such elements to develop and provide interoperable services)
- *Rent-seeking and other opportunistic pricing practices* (e.g., charging fees to provide interoperability services that exceed actual costs incurred to provide the services)
- *Non-standard implementation practices* (e.g., choosing not to adopt relevant standards, implementation specifications, and certification criteria)

Exceptions

1. Engaging in practices that prevent harm
2. Engaging in practices that protect the privacy of EHI
3. Implementing measures to promote the security of EHI
4. Recovering costs reasonably incurred
5. Declining to provide access, exchange, or use of EHI if a request is infeasible
6. Licensing technologies or other interoperability elements that are necessary to enable access to EHI
7. Making health IT unavailable to perform maintenance or improvements

Criteria for Workgroup Review

- *ONC basis* for selecting exceptions:
  - Each is limited to certain activities that *clearly advance the aims* of the information blocking provision
  - Each addresses a *significant risk that regulated actors will not engage in these beneficial activities* because of uncertainty concerning the breadth or applicability of the information blocking provision
  - Each is *subject to strict conditions* to ensure that it is limited to activities that are reasonable and necessary
- *Impact* of a practice and exception
- *Likely benefit* per Congressional intent and by actor/party
- *Implementation*: feasibility & complexity, cost & burden: by actor/party
- *Compliance: challenges*, uncertainties, potential best practices
- *Unintended consequences*

Actors and Other Definitions

Actors and Other Definitions: Findings §171.102

- The definition of an *actor* is critical because it exposes organizations to penalties and the regulatory implications of defined *practices* and *exceptions*.
- The proposed definition of an *HIN* is too broad and could include organizations that are not networks; it should be more narrowly focused:
  - For example, health plans, technology companies that handle *EHI*, and standards developing organizations (SDOs) or organizations that develop recommended interoperability polices are not networks and could, inappropriately, be included in the proposed definition.
  - Should receipt of health IT incentive program payments or federal stimulus payments be a determinant of whether an organization is an HIE or an HIN?
- The definition of an *HIE* includes *individuals*, which is difficult to understand, and, as with the *HIN* definition, could sweep in individuals or organizations that are not actually HIEs.
- The distinction between HIEs and HINs is unclear; HIEs should be viewed as a subset of HINs; ONC should therefore consider combining the two types of actors into one combined definition.
- The HIT *developer* definition needs more clarity on whether its application includes all *interoperability elements* under the control of the developer.
  - In addition, the definition is too broad as it could bring in companies that only have one product certified against one or a very few criteria, for example a quality reporting module.
  - The definition would also seem to inappropriately include organizations like value-added resellers in its focus on "offers" certified health IT.
- ONC should consider defining EHI to equal PHI as defined by HIPAA.

Information Blocking Practices

Practices: Findings
§171.103 and p. 76165

- The definition of *interoperability elements* is very broad (beyond certified health IT) and interacts with the identified information blocking practices and actors (and other aspects of the information blocking requirements) to create a very broad and complex web of compliance risk.
- Although part of the Cures statute, the term "likely" in the regulatory definition of information blocking, without a commonly understood definition or one in the proposed rule is problematic.
  - It could lead to an ongoing a large number of commercially motivated allegations of information blocking, even without any actual blocking.
  - Actions and capabilities associated with patient matching might trigger the "likely" level of risk.
  - ONC should define "likely" as "highly probable," backed up with examples of actual information blocking.
- There is a need to allow for due diligence as distinct from simply delaying access and such diligence should not need an exception (e.g., the security exception) to avoid implicating or being judged as information blocking. The need to vet external locations of exchange includes but is not limited to apps (e.g. networks).
  - In lieu of a focus on "vetting" of apps and other points of exchange by providers, CARIN Alliance suggests a focus on apps needing to be "centrally registered" by an EHR or a health plan. This approach allows a light 'vetting' process of the app but also allows the app to gain access to all client end points following registration without providers needing or wanting to vet every app. https://www.carinalliance.com/wp-content/uploads/2019/02/CARIN_Private-and-Secure-Consumer-Directed-Exchange_021019.pdf
  - It would be desirable if there can be a central point where apps are certified/vetted to achieve efficiencies for plans/providers/Vendors/app developers. If organizations want to do other vetting, that would be permitted of course, but at minimum CMS and ONC should release a White List for apps that they have vetted, and preferably also a Black List from the FTC if there is not a full fledged certification process. There is concern from some participants that being simply "registered" with a plan will not determine if it is a legitimate request, from a legitimate organization, with a legitimate scope of data elements.

Practices: Findings §171.103 and p. 76165

- The focus on non-standard implementations, combined with the broad definitions of actors, could pose challenges for certain organization, such as clinical registries, which have historically needed some non-standard implementations to achieve their intended purpose. In addition, we ask ONC to provide additional examples of non-standard implementations beyond those on p. 7521, for when applicable adopted standards exist and when they do not.
- There should be “safe harbor” provisions for some practices without the need to use an exception with all of its specificity.
- The nature of this rule and the underlying issue being addressed is leading ONC to assume actors have bad intent, and to err on the side of ensuring that there are no loopholes for these bad actors to exploit. This approach is understandable, but it casts such a wide net that there is a strong chance of collateral damage and pulling in those who are acting in good faith. It should be possible to relax some of the language in the practices and exceptions (e.g., “all things at all times and if no alternatives”), perhaps language that references acting in good faith and an allowance for “one off” cases in a gray area.

Exceptions

Preventing Harm: Findings §171.201

- This is an important exception. The example of domestic abuse (p. 7525) is apt and reinforces the importance of this exception. We urge ONC to ensure that the exception as finalized fully addresses relevant examples, included those that may be suggested in comments (e.g., is the focus on physical harm too restrictive?). ONC should also provide additional examples in the Final Rule. It should especially consider the challenges that will be faced in tailoring exceptions to specific threats of harm.
- The proposed burden of proof is unreasonable and the need to demonstrate that a policy is sufficiently tailored is likely to create a costly compliance burden.
- ONC should be explicit in recognizing the need for deference to other state and federal laws, including consideration of implications from the recently enacted Support Act.
- ONC and OCR must rapidly develop detailed guidance for the field, especially in the absence of a body of case law that can guide compliance.
- Will available technology (e.g., EHRs) enable actors, such as providers, to document compliance with this and other specific exceptions and their detailed components, including "and" and "or" scenarios. Will compliance tracking technology need to be validated?

Protecting Privacy: Findings §171.202

- Despite the OCR guidance on the HIPAA right of access and apps, there is a broad view that providers and developers will feel a need and obligation for some due diligence regarding apps and points of exchange.
  - A recent 2019 Manatt and eHealth Initiative Issue Brief *Risky Business? Sharing Data with Entities Not Covered by HIPAA* highlights existing international , federal and state laws, regulation and guidance and the highly complex and confusing environment that healthcare-related organizations face with respect to privacy and security related rights and obligations.
- ONC needs to be more realistic about the complexities and challenges of separating out 42 CFR Part 2 data from other EHI, especially but not only when the information is contained in clinical notes.
- There are important overlaps between privacy and security that must be recognized. There is concern that the proposed exceptions do not sufficiently recognize the kinds of bad actors that are present in the environment. For example, organizations that employ security-related attacks on other organizations vs. those that may have received authorization to access data but may collect more than authorized or use the information in unauthorized ways. It is essential that the exception enables actors to address the range of such security threats, including those posed by state actors.
- HHS should clarify when existing contractual obligations (as opposed to the decision to enforce such a provision), notably via BAAs, supersede Information Blocking provisions or provide a basis for an exception. We expand on this issue in comments in the "infeasible requests" exception.

Protecting Security: Findings §171.203

- APIs employed using appropriate standards and technologies and operational best practices can be very secure. In the final rule, ONC should be clear on this point as well as the necessary technologies and practice to achieve such security.
- ONC should confirm that cross-organizational sharing (e.g., provider to provider) of security information, regarding a state-sponsored threat or other "bad actor," is permissible and does not implicate information blocking or could fall within the indicated exception.
- ONC should confirm that an organization can use security policies that exceed what is required by law or regulation based on their assessment of the threat environment, without violating this exception.
- ONC should recognize the valid need to allow for due diligence as distinct from simply delaying access and such due diligence should not need the security exception to avoid implicating or being judged as engaged in information blocking. The need for vetting of external locations of exchange includes but is not limited to apps. (e.g. networks).

Protecting Security: Findings §171.203

- Despite the OCR guidance on the HIPAA right of access and apps, there is a broad view that providers and developers will feel a need and obligation for some due diligence regarding apps and points of exchange.
  - A recent 2019 Manatt and eHealth Initiative Issue Brief *Risky Business? Sharing Data with Entities Not Covered by HIPAA* highlights existing international , federal and state laws, regulation and guidance and the highly complex and confusing environment that healthcare-related organizations face with respect to privacy and security related rights and obligations.
- The security exception has a safety valve for cases where there is no written policy (171.203(e)). The exception calls for not only a determination that the practice is necessary, but that effectively there exists no other way of having protected your security that might have been less likely to interfere with information access. This requirement is asking a lot of the network engineers who may be trying to fight off a sustained attack at 3:00 am. We suggest that 171.203(e)(2) should therefore have a further safety valve for short-lived actions that are taken in good faith while a situation is being evaluated and understood.
- ONC should address the extent to which actions by an actor to address legal liability not mitigated by HHS Office of Civil Right (OCR) HIPAA-related policies can support use of this exception, including potential liability that can come with exchange that is not covered by OCR guidance relating to the HIPAA patient right of access. Such liability could arise from such sources as state laws, FTC regulations, or contractual obligations.

Recovering Costs Reasonably Incurred: Findings §171.204

- There was strong support for ONC's proposal to provide free API access to an individual who requests access to their EHI through a consumer-facing application and ONC should consider whether this approach could be extended to public health access.
- There were varying views regarding prohibition of fees for patient access:
  - Some noted that prohibition on any fees that do not meet this very detailed exception is too complex (both preamble and regulatory text) and interferes too much with market operations and could reduce investment in needed interoperability solutions. They suggest that ONC revise the exception to shift from an emphasis on cost recovery to a focus on the shared goal, central to 21st Century Cures, that pricing should not be a deterrent to information sharing.
  - Some also were concerned with the breadth of the prohibition on fees "based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's electronic health information.," particularly the reference to "designees." They noted that data accessed in this way by commercial "designees" (e.g., apps) has economic value with costs associated with its provision. Prohibiting any such fees to designees (as opposed to the individual) as part of the information blocking provision, beyond API certification requirements, could reduce investment in interoperability capabilities and overall availability of information. In addition, this issue has important interaction effects with the companion CMS interoperability proposed rule if payers, who are required and encouraged to create APIs are unable to recover costs because they have been defined as HIEs or HINs as part of this rule.
- There was concern with a high burden for hospitals to comply with this exception.

Recovering Costs Reasonably Incurred: Findings §171.204

- We ask ONC to clarify what individuals and entities are subject to the prohibition of fees for individual access and how to determine if an entity is actually an individual's designees for data sharing. More generally we ask ONC to clarify whether consent to share information to be interpreted as equivalent to actual patient direction to share?
- Many terms in this exception are subjective (e.g., "reasonable). We ask ONC to provide clear definitions in the final rule and associated guidance.
  - In particular, we ask ONC to provide more guidance on the allowance for "reasonable profit" in the preamble (p. 7538) and to explicitly include such an allowance in the regulatory text.
- ONC states that the method to recover costs "[m]ust not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic health information, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of electronic health information." The preamble (p. 7539) further states that "such revenue-sharing or profit-sharing arrangements would only be acceptable and covered by the exception if such arrangements are designed to provide an alternative way to recover the costs reasonably incurred for providing services." *The term "alternative" is confusing and could be read to imply that this method is an alternate to another simultaneously offered method of cost recovery, which we do not believe is ONC's intent; we ask ONC to clarify.*

Recovering Costs Reasonably Incurred: Findings §171.204

- The disallowance for costs that are "due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using electronic health information" requires further clarification. In particular, ONC should recognize that there are often multiple actors and actor-types involved in an implementation. A given actor could face higher costs as a result of non-standard implementations by another actor (e.g., a provider, a developer or vice versa). Such costs incurred as a result of non-standard design or implementation by another actor should be able to be reflected in fees.
- This exception should be expanded to clarify that costs associated with research, including costs from non-standard implementations due to research needs, should be able to be reflected in fees.
- There was interest and uncertainty as to how rapidly useful pricing information can be included in this exception.

Infeasible Requests: Findings §171.205

- We are very concerned that this exception is too vague, with many undefined terms (e.g., timely, burdensome, etc.). This vagueness will create uncertainty as to whether claiming this exception will ultimately be validated by regulators and therefore lessen the benefit of this important exception.
- We ask ONC to address potential conflicts between valid contracts, such as HIPAA Business Associate Agreements, and requests for data access that are inconsistent with these contracts. To what extent does the need to honor (as opposed to the desire to enforce) contractual obligations meet the infeasibility exception? ONC indicates in multiple places that actors cannot enforce certain contracts that are contrary to the provisions in this rule but does not address corresponding contractual obligations to honor contracts; this gap is very problematic, especially as application of these provisions will often require case-by case, fact-based evaluations.
- We ask ONC to recognize that infeasibility can come from the *scale effects* of requests for access as opposed to the marginal cost of meeting any given request (e.g., not tens of requests but tens of thousands of requests). Organizations may need to develop and uniformly apply policies to reflect the feasibility of types of requests and development and application of such policies should meet this exception so long as they meet criteria such as being non-discriminatory.

Infeasible Requests: Findings §171.205

- We ask ONC to recognize that honoring specific requests for information can be infeasible if the cost to meet that request, for example researching whether a patient has provided consent, are prohibitive.
- We ask ONC to confirm that infeasibility could include not having the technical capability in production to meet a request (e.g., not having APIs or other technical means to support a specific type of exchange, access, or use, for example to enable write access to the EHR), when the cost of acquiring such capabilities are excessive and could reduce the ability to meet other project plans and customer commitments.
- We ask ONC to consider whether a request can be deemed infeasible if there is another widely accepted alternative for performing the same or comparable action?
- We do not believe that this exception should need to be invoked, or information blocking implicated, if, per the regulatory language, the actor works "with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information".
- We ask ONC to confirm lack of backwards compatibility of standards could be a basis for invoking this exception, for example if ONC finalizes its proposal to allow both FHIR DSTU 2 and FHIR Release 4.

Reasonable and Non-Discriminatory Terms (RAND) Licensing: Findings §171.206

- Overall, we ask ONC to simplify this exception and its scope and to provide more guidance on RAND licensing and its implementation.
- We request that ONC address the potential for unintended consequences; for example, some health IT delivery models might have fees eligible for the RAND licensing exception and others would only eligible for 171.204, with the potential for higher net financial returns under one model or the other, a preference that is not intended (and should not be) as a matter of public policy.
- The preamble discussion of this exception is complex and will require very technical and fact-specific steps by actors, including establishment of "reasonable" royalties.
- We ask ONC to consider the combined implications and timing to assess feasibility, licensing implications and enter a negotiation for licensing within a 10-day timeframe.

Reasonable and Non-Discriminatory Terms (RAND) Licensing: Findings §171.206

- In addition, given the extensive use of licenses as one element of commercial health IT software offerings, we ask ONC to clarify which software licenses would need to (be revised to) meet this exception to avoid information blocking (i.e., will *all* software licenses need to be converted to RAND terms or only those that focus on specific intellectual property rights, and in what timeframe?). For example, would licenses for EHRs presented to providers be subject to this provision or only licenses for specific IP (e.g., code sets) or APIs licensed by an EHR developer to an application developer? We also ask ONC to recognize that this exception, if it requires changes to virtually all health IT software licenses, is likely to have far reaching and very disruptive impacts on the market for health IT software, including a high compliance and documentation burden.
- We ask ONC to clarify its definition of "royalty" and which fees associated with licenses software would be consider a royalty and which would not, and hence only eligible for the exception at 171.204.

Reasonable and Non-Discriminatory Terms (RAND) Licensing: Findings §171.206

- We ask ONC to clarify whether*, in all cases*, fees that might be associated with software are also eligible for the alternate exception under 171.204. The preamble (p. 7549) states that "[f]inally, the actor must not condition the use of interoperability elements one requirement or agreement to pay a fee of any kind whatsoever unless the fee meets either the narrowly crafted condition to this exception for a reasonable royalty, or, alternatively, the fee satisfies the separate exception proposed in § 171.204, which permits the recovery of certain costs reasonably incurred".
- We also ask ONC to clarify whether an actor that licenses an interoperability element, and chooses to use the exception at 171.204 for fees, would also need to use this exception, as there are many non-monetary aspects of this exception.
- We ask ONC to address an actor's obligation to license intellectual property that they do not yet have and to clarify that inability to honor such a request could be met by the feasibility exception and would not require use of this one as well.

Health IT Performance: Findings §171.207

- We ask ONC to recognize that it is unlikely that actors would make a system unavailable as part of deliberate information blocking and we question whether such downtime should be considered a practice that implicates information blocking and hence, whether this exception is needed.
  - Providers have strong incentives to keep systems up and to respond quickly to unplanned outages
- We recognize that system unavailability due to prevention of harm or security risks would fall under those exceptions and not this one. At the same time, subjecting urgent system downtime needs to the far-reaching requirements associated with *any* of these exceptions seems unwarranted.
- The language in this exception (preamble and regulation) is not sufficiently clear.
  - For example, what if only one part of a system goes down, such as the gateway for inbound queries?

Health IT Performance: Findings §171.207

- In general, unplanned *maintenance* would not occur. We ask ONC to recognize that unplanned downtime will almost always only occur when the actor initiating the downtime is unable to control such situations.
- Scheduling downtime is very complex even within an organization; the need to gain the assent of external parties affected by the downtime is impractical and infeasible.
  - Consider a cloud-based system that is used by hundreds or thousands of users. Would the actor be unable to initiate needed maintenance if even one of these users did not agree?
  - We agree that it is desirable for service level agreements (SLAs) to address maintenance downtime but requiring agreement by users for *any* downtime should not be required.
  - If ONC makes needed system maintenance and upgrades more difficult to accomplish, overall system quality will be threatened.

Requests for Information—Disincentives for Health Care Providers: Findings (p. 7553)

- We do not believe that additional provider disincentives are needed given those already in place.

Next Steps

- The Information Blocking Workgroup will continue its work following submission of comments to ONC.
- This ongoing work will include:
  - Assessments of proposed rule implications to the community; and
  - Discussions to clarify information blocking policies and considerations, including follow-up actions needed from the federal government and private sector, prior to and after the Final Rule.