Information Blocking Workgroup

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

Interoperability Matters

4/30/2019

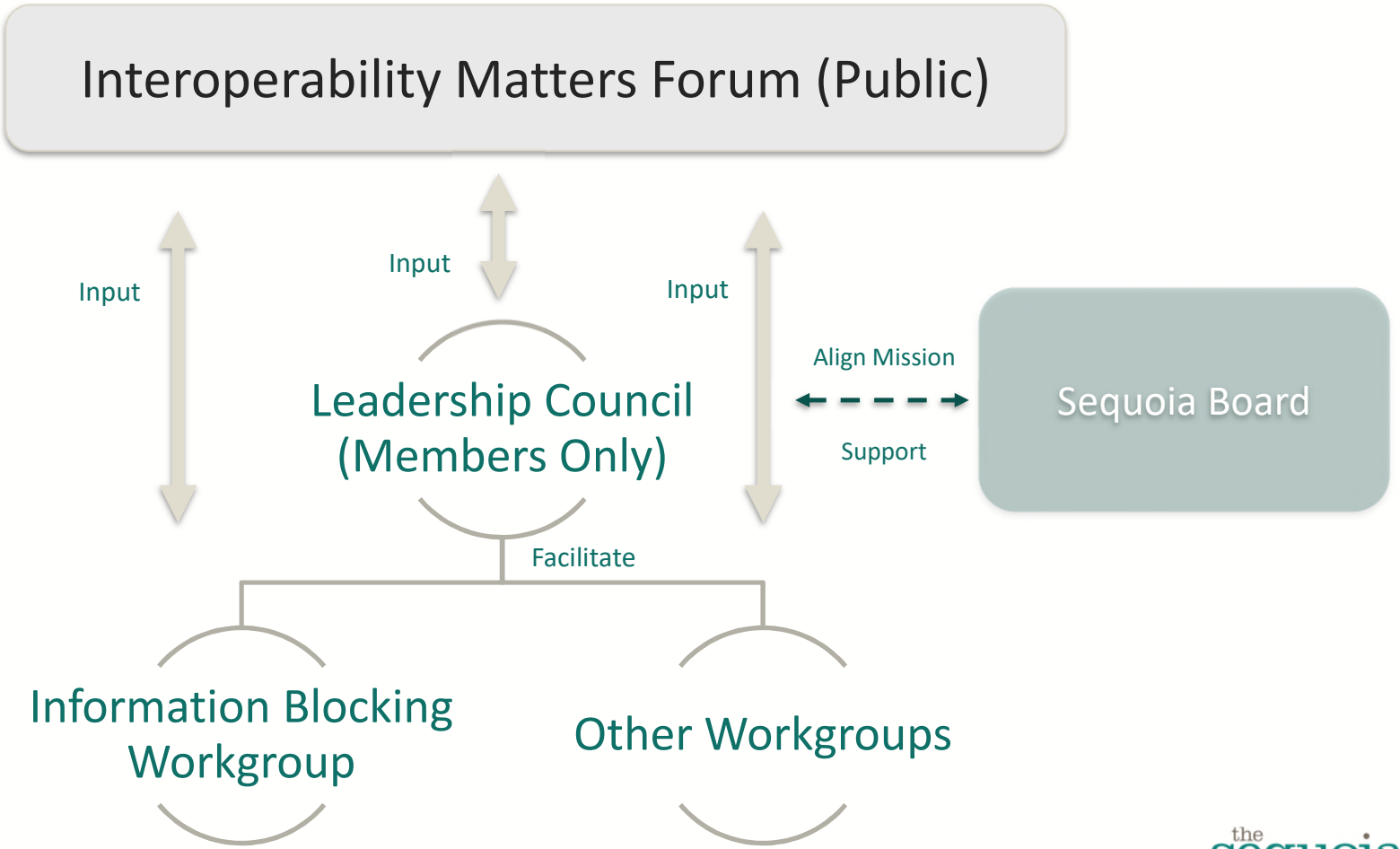
Organization of the Report

- 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.