Information Blocking Workgroup

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

Presented to:

Interoperability Matters Leadership Council

4/22/2019

the sequoia project

Agenda

- Welcome
- Leadership Council Role
- Context: Cooperative Process
- Criterial for Successful Work Group Process
- Information Blocking Work Group Overview
- Organization of the Report
- Information Blocking Work Group Final Report
- Lessons Learned
- Next Steps

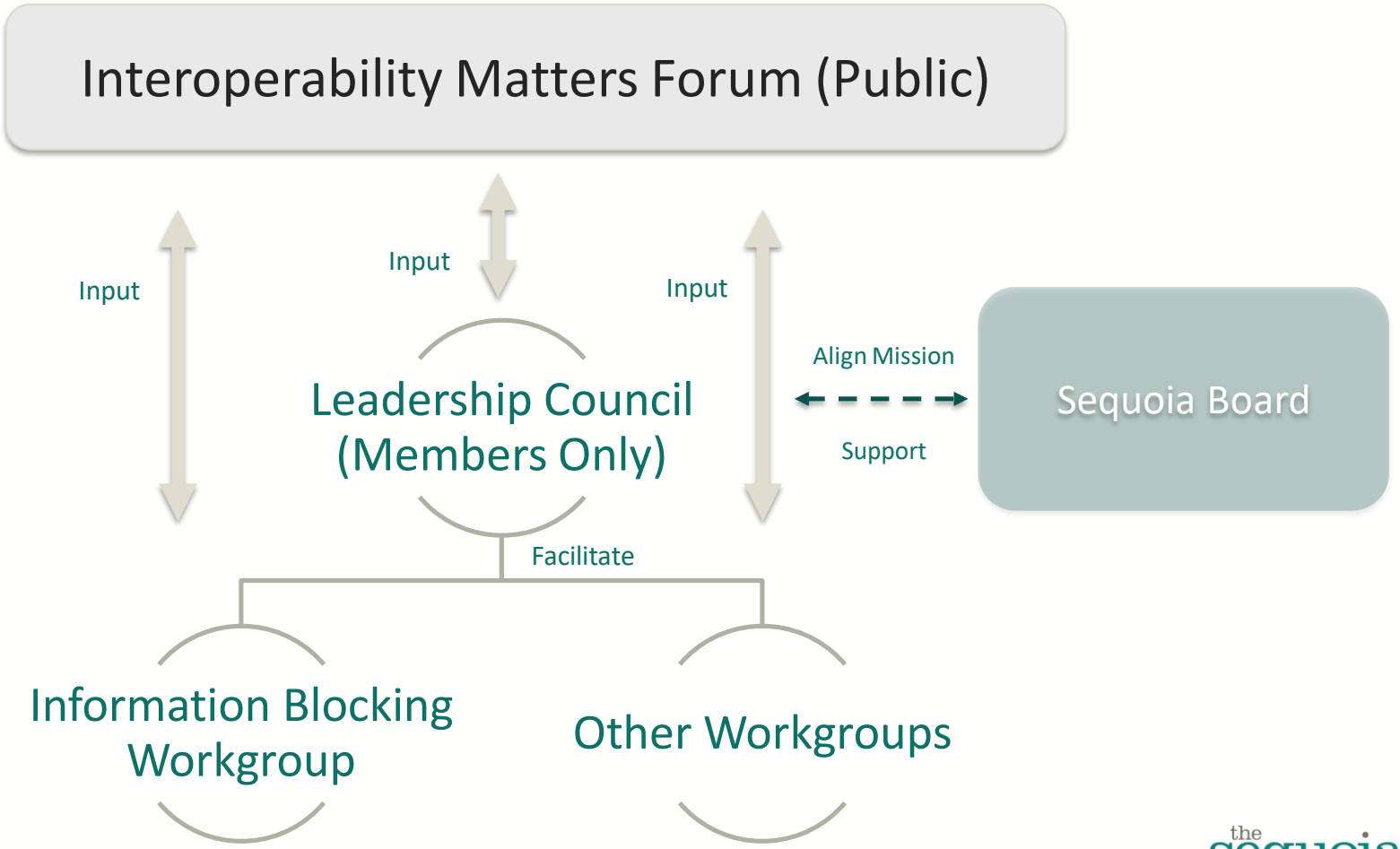
Leadership Council Role

- Understand the process that produced the report
- Accept the report, which reflects the process
- Uncover learnings
- Advise regarding changes / refinements to the process
- Support the next phase of the Work Group

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

Criteria for a Successful Work Group Process

- Charter and scope of work is clear
- Representation is sufficiently broad and diverse to cover a balanced range of perspectives
- Members are actively engaged
- Subject matter experts prepare discussion materials
- Sufficient staff and organizational support
- Sufficient time for member consideration and input
- Discussion structured in a way to elicit feedback on most salient issues
- Timely and productive facilitated calls
- Feedback reflected in updated discussion materials

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

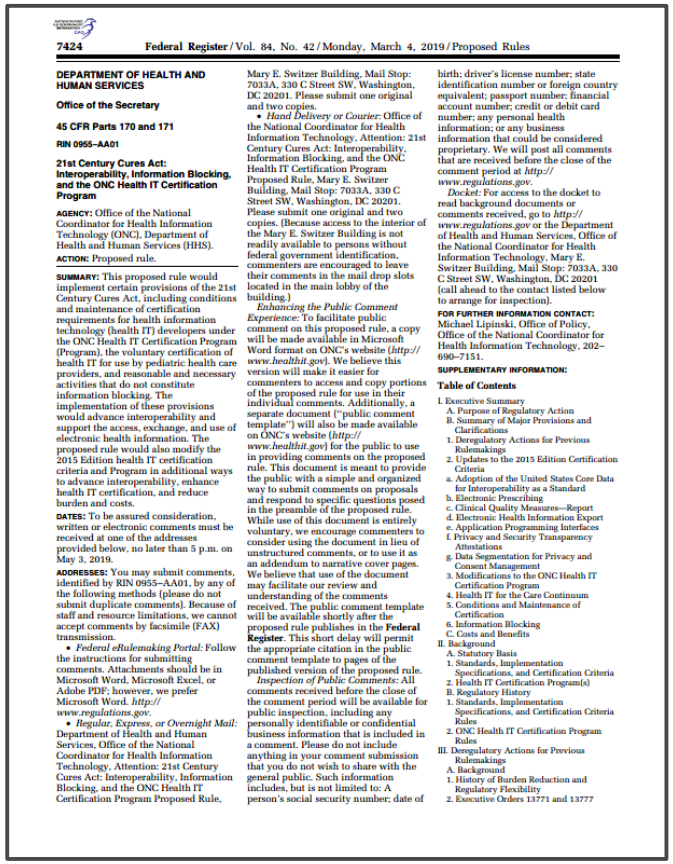
Informatics
- Doug Fridsma, AMIA

Safety net providers / service provider
- Jennifer Stoll, OCHIN

Release of Information Company
- Rita Bowen, MROCorp

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*

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

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 were varying views regarding prohibition of fees for patient access:
- 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.
  - 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.
- Overall, we ask ONC to simplify this exception and its scope and to provide more guidance on RAND licensing and its implementation.

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 request that ONC address the potential for unintended consequences; for example, some types of 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.

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

- 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.
- 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, for example 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.

Opportunities for Future Work Group Efforts

- Provide an opportunity early on for the Workgroup to suggest project scope refinements to the Leadership Council
- Consider longer, less frequent calls (e.g. 90 minutes) to provide more time for interactive dialogue
- Provide additional mechanisms to encourage interaction (e.g. phone dialogue, web meeting chat, other online forum, other web meeting features)
- Support open office hours for participants to ask questions and share feedback outside of a large group setting
- Consider 1:1 outreach for certain matters (e.g. certain topics which have sensitivity, e.g. licensing)
- Use targeted questions or pre-plan to have 2 work group members share their views on a topic to encourage interactive discussion

Background

Key Milestones

Confirmed Times and Registration for Leadership Council & Public Calls will be posted at https://sequoiaproject.org/interoperability-matters/information-blocking-workgroup-public-advisory-forum/

Information Blocking Workgroup Meeting #4

Interoperability Matters

4/15/2019

the sequoia project

Agenda

- Welcome and Introductions
- Review Draft Findings
  - Actors and Other Definitions
  - 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
  - Conditions & Maintenance of Certification: Information Blocking
  - RFIs: disincentives for providers and price transparency
  - Complaints and enforcement
- Public Input
- Closing

Workgroup Representatives

Associations and Orgs - health IT community
- Tom Leary / 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

**Invited*

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, Johns Hopkins University

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

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 Defined §171.102

Health Care Providers	Same meaning as "health care provider" at 42 U.S.C. 300jj—includes hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, Federally qualified health center, group practice, pharmacist, pharmacy, laboratory, physician, practitioner, provider operated by, or under contract with, the IHS or by an Indian tribe, tribal organization, or urban Indian organization, rural health clinic, a covered entity ambulatory surgical center, therapist, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.
Health IT Developers of Certified Health IT	An individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program
Health Information Exchanges	Individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes
Health Information Networks	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

HIEs and HINs

HIE

- Include but not limited to RHIOs, state HIEs, other organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used between or among particular types of parties or for particular purposes
- Might facilitate or enable access, exchange, or use exclusively within a region, or for a limited scope of participants and purposes (e.g., registry or exchange established by hospital-physician organization to facilitate ADT alerting)
- May be established for specific health care or business purposes or use cases
- If facilitates access, exchange, or use for more than a narrowly defined set of purposes, may be HIE and a HIN

HIN

- Entity established in a state to improve movement of EHI between providers operating in state; identifies standards for security and offers Ts and Cs for providers wishing to participate in the network.
- Entity offering (and overseeing and administering) Ts and Cs 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 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
- Note: Network is never defined

Are distinctions clear? Too broad or too narrow? Consistent with congressional intent?

Actors and Other Definitions: Preliminary Findings

- 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 on 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

Information Blocking Practices

Cures Statute

- (A) practices that restrict authorized *access*, *exchange*, or *use* under applicable State or Federal law of such information for *treatment and other permitted purposes* under such applicable law, including transitions between certified health information technologies;
- (B) implementing health information technology in *nonstandard* ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information;
- (C) implementing health information technology in ways that are likely to— "(i) restrict the access, exchange, or use of electronic health information with respect to *exporting complete information sets* or in *transitioning between health information technology systems*;
- or "(ii) lead to fraud, waste, or abuse, or *impede innovations and advancements* in health information access, exchange, and use, including care delivery enabled by health information technology.

Proposed Rule

- 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)*

ONC examples in Background. Too broad or too narrow? Consistent with congressional intent?

Practices: Preliminary Findings

- 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 specific 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 suggest 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.
- 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.
- There should be "safe harbor" provisions for some *practices* without no 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

Exception: Preventing Harm

- An actor may engage in practices that are reasonable and necessary to prevent *harm* to a patient or another person
- The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm (special focus on physical harm) to a patient or another person
- The practice must implement an *organizational policy* that meets certain requirements *or* must be based on an *individualized assessment of the risk in each case*

42 CFR Part 2 and ability to isolate records that could lead to harm (e.g., in notes).
Is the focus on physical harm appropriate?

Preventing Harm: Preliminary Findings

- 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
- 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 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 specific exceptions and their detailed components, including “and” and “or” scenarios. Will compliance tracking technology need to be validated?

Exception: Promoting the Privacy of Electronic Health Information

- An actor may engage in practices that protect the privacy of EHI
- An actor must satisfy *at least one of four* discrete sub-exceptions that address scenarios that recognize existing privacy laws and privacy-protective practices:
  1. Practices that satisfy preconditions prescribed by privacy laws;
  2. Certain practices not regulated by HIPAA but that implement documented and transparent privacy policies;
  3. Denial of access practices that are specifically permitted under HIPAA; or
  4. Practices that give effect to an individual's privacy preferences.
- Actors need not provide access, exchange, or use of EHI in a manner not permitted under the HIPAA Privacy Rule
- General conditions apply to ensure that practices are tailored to the specific privacy risk or interest being addressed and implemented in a *consistent and non-discriminatory manner*

Are non-HIPAA entities sufficiently addressed?
Organizational policies (some could be information blocking practice; others could enable exception)

Protecting Privacy: Preliminary Findings

- 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.

Exception: Promoting the Security of Electronic Health Information

- An actor may implement measures to promote the security of EHI
  - The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI
  - The practice must be tailored to specific security risks and must be implemented in a consistent and non-discriminatory manner
  - The practice must implement an organizational security policy that meets certain requirements or must be based on an individualized determination regarding the risk and response in each case

Are non-HIPAA entities sufficiently addressed?
Organizational policies (some could be information blocking practice; others could enable exception)

Protecting Security: Preliminary Findings

- 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).
- 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 an awful lot of the network engineers who may eb trying to fight off a sustained attack at 3:00 am. 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 avoid legal liability beyond specific 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.

Exception: Recovering Costs Reasonably Incurred

- An actor may recover costs that it reasonably incurs, in providing access, exchange, or use of EHI
- Fees must be:
  - charged on the basis of *objective and verifiable criteria uniformly applied* to all similarly situated persons and requests;
  - *related to the costs* of providing access, exchange, or use; and
  - *reasonably allocated among all customers* that use the product/service
  - Must not be based in any part on whether requestor is a *competitor*, potential competitor, or will be using EHI to facilitate competition with the actor; and
  - Must not be based on *sales, profit, revenue*, or other value that the requestor derives or may derive *that exceed the actor's reasonable costs*
- Fees must not be based on *anti-competitive* or other impermissible criteria
- Certain costs would be excluded from this exception, such as costs that are *speculative or subjective* or *associated with electronic access by an individual to their EHI*

Issues: Documentation? "Related" to costs vs. equal to costs? Profit – not in regulatory language? Unintended consequences?

Recovering Costs : Preliminary Findings

- There were varying views regarding prohibition of fees:
  - 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.
  - 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.
- 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." In the preamble (p. 7539), it 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 this method is an alternate to another simultaneously offered method of cost recovery, which we do not believe to be ONC's intent. We ask ONC to clarify its intent.

Recovering Costs : Preliminary Findings

- 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.

Exception: Responding to Requests that are Infeasible

- An actor may decline to provide access, exchange, or use of EHI in a manner that is *infeasible*
- Complying with the request must impose a *substantial burden on the actor that is unreasonable under the circumstances* (taking into account the cost to the actor, actor's resources, etc.)
- The actor must *timely respond* to infeasible requests

Likely scenarios? Too broad or too narrow?

Infeasible Requests: Preliminary Findings

- 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: Preliminary Findings

- 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".

Exception: Licensing Interoperability Elements on Reasonable and Non-Discriminatory Terms

- An actor that controls technologies or other interoperability elements that are necessary to enable access to EHI will not be information blocking so long as it licenses such elements on *reasonable and non-discriminatory terms (RAND)*
  - RAND terms often used by SDOs
- The license can impose a *reasonable royalty* but *must include appropriate rights* so that the licensee can develop, market, and/or enable the use of interoperable products and services
- License terms must be based on *objective and verifiable criteria* that are *uniformly applied and must not be based on impermissible criteria*, such as whether the requestor is a potential competitor

Issues: Documentation? Unintended consequences? "Reasonable"? Scope of this requirement – EHRs?

RAND Licensing: Preliminary Findings

- The preamble discussion of this exception is complex and will require very technical and fact-specific steps by actors, including establishment of "reasonable" royalties.
- 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.
- 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 types of 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.

RAND Licensing: Preliminary Findings

- 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.
- 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 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.
- 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.

Exception: Maintaining and Improving Health IT Performance

- An actor may make health IT under its control temporarily unavailable to perform maintenance or improvements to the health IT
- The actor to whom health IT is provided must agree to unavailability, via service level agreement (SLA) or similar agreement or in each event
  - Obligations differ if health IT vendor or provider
- An actor must ensure that the health IT is unavailable for no longer than necessary to achieve the maintenance or improvements

How practical will notification be for unplanned downtime. Can SLAs meet this requirement?

Health IT Performance: Preliminary Findings

- 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.
- 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 given the other points in these comments.
- The language in this exception (preamble and regulation) is not sufficiently clear.
- 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.
- More generally, scheduling downtime is very complex even within an organization; the need to gain the assent of *every* party 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.

Final Topics

Maintenance of Certification: Information Blocking

- Per Cures, ONC proposes Conditions and Maintenance of Certification requirements for the ONC Health IT Certification Program – some relate directly or indirectly to information blocking*
  - Information Blocking*
  - Assurances *
  - Communications
  - Application Programming Interfaces (APIs)*
  - Real World Testing
  - Attestations*
  - (Future) Electronic Health Record (EHR) Reporting Criteria Submission

Note: *In some cases, such as API pricing, criteria are more stringent than general information blocking provisions (e.g., fee record keeping) but must also be met to also satisfy information blocking exceptions.*

Information Blocking/Certification: Preliminary Findings

Requests for Information

- Additional Exceptions
  - Whether 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)—*Not a safe harbor*
  - ONC welcomes comment on any potential new exceptions for future rulemaking
- Disincentives for Health Care Providers
  - ONC asks if new disincentives or if modifying disincentives already available under HHS programs and regulations (e.g., provider attestations under incentive programs) would provide more effective deterrents

Any new exceptions needed? Additional provider disincentives?

RFIs: Preliminary Findings

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

Complaint Process and Enforcement

- Section 3022(d)(3)(A) of PHSA directs ONC to implement a standardized process for the public to submit claims of information blocking
  - ONC intends to implement and evolve this complaint process by building on existing mechanisms, including the complaint process available at https://www.healthit.gov/healthit-feedback
- ONC requests comments on this approach and any alternative approaches that would best address this aspect of Cures
- ONC also requests comment on several issues in proposed rule
- Enforcement primarily by ONC and OIG (limited role for ACBs)

Is complaint and enforcement process clear?

Complaint and Enforcement: Preliminary Findings

Next Steps

- A draft report from this call will be sent to the Workgroup by April 16
  - High level recommendations
  - Comments due back by Close of Business April 17
    - Please focus on major concerns or suggested clarifying edits
    - interopmatters@sequoiaproject.org—Reference "Workgroup" in header
- Leadership Council to receive a report from the Work Group on April 22
- Sequoia Board to receive a report from the Leadership Council on April 26
- Comments to ONC by May 3
- Thank you all!

Information Blocking Workgroup Meeting #3

Interoperability Matters

4/3/2019

the sequoia project

Agenda

- Welcome and Introductions
- Exceptions
    4. Recovering costs reasonably incurred
    5. Declining to provide access, exchange, or use of EHI if request is infeasible
    6. Licensing technologies or other interoperability elements
    7. Making health IT unavailable to perform maintenance or improvements
- Conditions & Maintenance of Certification: Information Blocking
- RFIs: disincentives for providers and price transparency
- Complaints and enforcement
- Next Steps

Workgroup Representatives

Associations and Orgs - health IT community
- Tom Leary / 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

**Invited*

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, Johns Hopkins University

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

Rules of the Road

- We want to hear from you!
- Let's focus on highest priority points and themes
- We encourage use of chat during the meeting to make points and we will capture the chat logs
- Send us your thoughts between meetings
  - interopmatters@sequoiaproject.org
  - Reference "Workgroup" in message header

Exception: Recovering Costs Reasonably Incurred

- An actor may recover costs that it reasonably incurs, in providing access, exchange, or use of EHI
- Fees must be:
  - charged on the basis of *objective and verifiable criteria uniformly applied* to all similarly situated persons and requests;
  - *related to the costs* of providing access, exchange, or use; and
  - *reasonably allocated among all customers* that use the product/service
  - Must not be based in any part on whether requestor is a *competitor*, potential competitor, or will be using EHI to facilitate competition with the actor; and
  - Must not be based on *sales, profit, revenue*, or other value that the requestor derives or may derive *that exceed the actor's reasonable costs*
- Fees must not be based on *anti-competitive* or other impermissible criteria
- Certain costs would be excluded from this exception, such as costs that are *speculative or subjective* or *associated with electronic access by an individual to their EHI*

Issues: Documentation? "Related" to costs vs. equal to costs? Profit – not in regulatory language? Unintended consequences?

Exception: Recovering Costs Reasonably Incurred

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Types of costs to which this exception applies*. This exception is limited to the actor's costs reasonably incurred to provide access, exchange, or use of electronic health information.

(b) *Method for recovering costs*. The method by which the actor recovers its costs—

(1) Must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests;

(2) Must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged;

(3) Must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported;

(4) Must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor; and

(5) Must 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.

(c) *Costs specifically excluded*. This exception does not apply to—

(1) Costs that the actor incurred 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;

(2) Costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets;

(3) Opportunity costs, except for the reasonable forward-looking cost of capital;

(4) A fee prohibited by 45 CFR 164.524(c)(4);

(5) A fee 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;

(6) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; **or**

(7) A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

(d) *Compliance with the Conditions of Certification*. (1) Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4) or § 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

(2) If the actor is an API Data Provider, the actor is only permitted to charge the same fees that an API Technology Supplier is permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification in § 170.404 of this subchapter.

Recovering Costs : Recommendations

Exception: Responding to Requests that are Infeasible

- An actor may decline to provide access, exchange, or use of EHI in a manner that is *infeasible*
- Complying with the request must impose a *substantial burden on the actor that is unreasonable under the circumstances* (taking into account the cost to the actor, actor's resources, etc.)
- The actor must *timely respond* to infeasible requests

Likely scenarios? Too broad or too narrow?

Exception: Responding to Requests that are Infeasible

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Request is infeasible*. (1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—

(i) The type of electronic health information and the purposes for which it may be needed;

(ii) The cost to the actor of complying with the request in the manner requested;

(iii) The financial, technical, and other resources available to the actor;

(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;

(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request;

(vii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; **and**

(viii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.

(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.

(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(b) *Responding to requests*. The actor must timely respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements.

(c) *Written explanation*. The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(d) *Provision of a reasonable alternative*. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information.

Infeasible Requests: Recommendations

Exception: Licensing Interoperability Elements on Reasonable and Non-Discriminatory Terms

- An actor that controls technologies or other interoperability elements that are necessary to enable access to EHI will not be information blocking so long as it licenses such elements on *reasonable and non-discriminatory terms (RAND)*
  - RAND terms often used by SDOs
- The license can impose a *reasonable royalty* but *must include appropriate rights* so that the licensee can develop, market, and/or enable the use of interoperable products and services
- License terms must be based on *objective and verifiable criteria* that are *uniformly applied and must not be based on impermissible criteria*, such as whether the requestor is a potential competitor

Issues: Documentation? Unintended consequences? "Reasonable"? Scope of this requirement – EHRs?

Exception: Licensing Interoperability Elements on Reasonable and Non-discriminatory Terms

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Responding to requests*. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:

(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; **and**

(2) Offering an appropriate license with reasonable and non-discriminatory terms.

(b) *Reasonable and non-discriminatory terms*. The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory.

(1) *Scope of rights*. The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.

(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.

(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.

(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(2) *Reasonable royalty*. If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements.

(i) The royalty must be non-discriminatory, consistent with paragraph (b)(3) of this section.

(ii) The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information.

(iii) If the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on reasonable and non-discriminatory terms, the actor may charge a royalty that is consistent with such policies.

Exception: Licensing Interoperability Elements on Reasonable and Non-discriminatory Terms

(3) *Non-discriminatory terms*. The terms (including royalty terms) on which the actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements.

(i) The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(ii) The terms must not be based in any part on—

(A) Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; **or**

(B) The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements, including the secondary use of such electronic health information.

(4) *Collateral terms*. The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following.

(i) Not compete with the actor in any product, service, or market.

(ii) Deal exclusively with the actor in any product, service, or market.

(iii) Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets the requirements of the exception in § 171.204.

(5) *Non-disclosure agreement*. The actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets, provided—

(i) The agreement states with particularity all information the actor claims as trade secrets; **and**

(ii) Such information meets the definition of a trade secret under applicable law.

(c) *Additional requirements relating to the provision of interoperability elements*. The actor must not engage in any practice that has any of the following purposes or effects.

(1) Impeding the efficient use of the interoperability elements to access, exchange, or use electronic health information for any permissible purpose.

(2) Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

(3) Degrading the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

(d) *Compliance with conditions of certification*. Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the conditions of certification in §§ 170.402, 170.403, or 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

RAND Licensing: Recommendations

Exception: Maintaining and Improving Health IT Performance

- An actor may make health IT under its control temporarily unavailable to perform maintenance or improvements to the health IT
- The actor to whom health IT is provided must agree to unavailability, via service level agreement (SLA) or similar agreement or in each event
  - Obligations differ if health IT vendor or provider
- An actor must ensure that the health IT is unavailable for no longer than necessary to achieve the maintenance or improvements

How practical will notification be for unplanned downtime. Can SLAs meet this requirement?

Exception: Maintaining and Improving Health IT Performance

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Maintenance and improvements to health IT*. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—

(1) For a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable;

(2) Implemented in a consistent and non-discriminatory manner; **and**

(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, *agreed to* by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.

(b) *Practices that prevent harm.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

(c) *Security-related practices*. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.

Health IT Performance: Recommendations

Maintenance of Certification: Information Blocking

- Per Cures, ONC proposes Conditions and Maintenance of Certification requirements for the ONC Health IT Certification Program – some relate directly or indirectly to information blocking*
  - Information Blocking*
  - Assurances *
  - Communications
  - Application Programming Interfaces (APIs)*
  - Real World Testing
  - Attestations*
  - (Future) Electronic Health Record (EHR) Reporting Criteria Submission

Note: *In some cases, such as API pricing, criteria are more stringent than general information blocking provisions (e.g., fee record keeping) but must also be met to also satisfy information blocking exceptions.*

Information Blocking/Certification: Recommendations

Requests for Information

- Additional Exceptions
  - Whether 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)—*Not a safe harbor*
  - ONC welcomes comment on any potential new exceptions for future rulemaking
- Disincentives for Health Care Providers
  - ONC asks if new disincentives or if modifying disincentives already available under HHS programs and regulations (e.g., provider attestations under incentive programs) would provide more effective deterrents

Any new exceptions needed? Additional provider disincentives?

RFIs: Recommendations

Complaint Process and Enforcement

- Section 3022(d)(3)(A) of PHSA directs ONC to implement a standardized process for the public to submit claims of information blocking
  - ONC intends to implement and evolve this complaint process by building on existing mechanisms, including the complaint process available at https://www.healthit.gov/healthit-feedback
- ONC requests comments on this approach and any alternative approaches that would best address this aspect of Cures
- ONC also requests comment on several issues in proposed rule
- Enforcement primarily by ONC and OIG (limited role for ACBs)

Is complaint and enforcement process clear?

Complaint Process: Recommendations

Final Thoughts and Next Steps

- Next meeting is April 15 with public invited to listen and comment at end
- There is also another public forum on April 5
- Please send any follow-up thoughts on topics addressed by April 5 if possible
  - interopmatters@sequoiaproject.org
  - Reference “Workgroup” in message header

Information Blocking Workgroup Meeting #2

Interoperability Matters

3/25/2019

the sequoia project

Agenda

- Welcome and Introductions
- Workgroup Overview Refresh
- Actors and Other Definitions
  - Providers
  - CEHRT Developers
  - HIEs
  - HINs
- Information Blocking Practices
- Exceptions
  - Harm
  - Privacy
  - Security
- Next Steps

Actors Defined §171.102 – Focus of WG #2

Health Care Providers	Same meaning as "health care provider" at 42 U.S.C. 300jj—includes hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, Federally qualified health center, group practice, pharmacist, pharmacy, laboratory, physician, practitioner, provider operated by, or under contract with, the IHS or by an Indian tribe, tribal organization, or urban Indian organization, rural health clinic, a covered entity ambulatory surgical center, therapist, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.
Health IT Developers of Certified Health IT	An individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program
Health Information Exchanges	Individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes
Health Information Networks	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

HIEs and HINs

HIE

- Include but not limited to RHIOs, state HIEs, other organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used between or among particular types of parties or for particular purposes
- Might facilitate or enable access, exchange, or use exclusively within a region, or for a limited scope of participants and purposes (e.g., registry or exchange established by hospital-physician organization to facilitate ADT alerting)
- May be established for specific health care or business purposes or use cases
- If facilitates access, exchange, or use for more than a narrowly defined set of purposes, may be HIE and a HIN

HIN

- Entity established in a state to improve movement of EHI between providers operating in state; identifies standards for security and offers Ts and Cs for providers wishing to participate in the network.
- Entity offering (and overseeing and administering) Ts and Cs 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 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
- Note: Network is never defined

Are distinctions clear? Too broad or too narrow? Consistent with congressional intent?

Actors: Recommendations

Information Blocking Practices

Cures Statute

- (A) practices that restrict authorized *access*, *exchange*, or *use* under applicable State or Federal law of such information for *treatment and other permitted purposes* under such applicable law, including transitions between certified health information technologies;
- (B) implementing health information technology in *nonstandard* ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information;
- (C) implementing health information technology in ways that are likely to— ‘‘(i) restrict the access, exchange, or use of electronic health information with respect to *exporting complete information sets* or in *transitioning between health information technology systems*;
- or ‘‘(ii) lead to fraud, waste, or abuse, or *impede innovations and advancements* in health information access, exchange, and use, including care delivery enabled by health information technology.

Proposed Rule

- 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)*

ONC examples in Background. Too broad or too narrow? Consistent with congressional intent?

Practice: Recommendations

Information Blocking: "Reasonable and Necessary" Exceptions

- If *practice* satisfies one or more exceptions, *actor* would not be treated as *information blocking* and not subject to penalties and disincentives
  - Most exceptions apply to all actors, unless otherwise indicated
- Consistent themes across exceptions (e.g., pro-competitive, consistent, non-discriminatory, policies in place and documented compliance with these policies)
- *Must generally meet all elements at all relevant times to satisfy an exception for each practice where an exception is claimed*
  - Rather than "substantial compliance" (e.g., HIPAA)
- The actor has the burden of proving compliance with the exception in the event of an investigation

ONC Policy Considerations for Exceptions

1. Each is limited to certain *activities that clearly advance the aims of the information blocking provision*
2. 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
3. Each is subject to *strict conditions to ensure that it is limited to activities that are reasonable and necessary*

Exception: Preventing Harm

- An actor may engage in practices that are reasonable and necessary to prevent *harm* to a patient or another person
- The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm (special focus on physical harm) to a patient or another person
- The practice must implement an *organizational policy* that meets certain requirements *or* must be based on an *individualized assessment of the risk in each case*

42 CFR Part 2 and ability to isolate records that could lead to harm (e.g., in notes).
Is the focus on physical harm appropriate?

Exception: Preventing Harm

To qualify for this exception, each practice by an actor must meet the following conditions at *all* relevant times.

(a) The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from—

(1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record;

(2) Misidentification of a patient or patient's electronic health information; **or**

(3) Disclosure of a patient's electronic health information in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

(b) If the practice implements an organizational policy, the policy must be—

(1) In writing;

(2) Based on relevant clinical, technical, and other appropriate expertise;

(3) Implemented in a consistent and non-discriminatory manner; **and**

(4) No broader than necessary to mitigate the risk of harm.

(c) If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm.

Preventing Harm: Recommendations

Exception: Promoting the Privacy of Electronic Health Information

- An actor may engage in practices that protect the privacy of EHI
- An actor must satisfy *at least one of four* discrete sub-exceptions that address scenarios that recognize existing privacy laws and privacy-protective practices:
  1. Practices that satisfy preconditions prescribed by privacy laws;
  2. Certain practices not regulated by HIPAA but that implement documented and transparent privacy policies;
  3. Denial of access practices that are specifically permitted under HIPAA; or
  4. Practices that give effect to an individual's privacy preferences.
- Actors need not provide access, exchange, or use of EHI in a manner not permitted under the HIPAA Privacy Rule
- General conditions apply to ensure that practices are tailored to the specific privacy risk or interest being addressed and implemented in a *consistent and non-discriminatory manner*

Are non-HIPAA entities sufficiently addressed?
Organizational policies (some could be information blocking practice; others could enable exception)

Exception: Promoting the Privacy of Electronic Health Information

To qualify for this exception, each practice by an actor must satisfy at least one of the sub-exceptions in paragraphs (b) through (e) of this section at all relevant times.

(a) *Meaning of "individual" in this section*. The term "individual" as used in this section means one or more of the following—

(1) An individual as defined by 45 CFR 160.103.

(2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(3) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g).

(4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual's estate under State or other law.

(b) *Precondition not satisfied.* If the actor is required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of electronic health information, the actor may choose not to provide access, exchange, or use of such electronic health information if the precondition has not been satisfied, provided that—

(1) The actor's practice—

(i) Conforms to the actor's organizational policies and procedures that:

(A) Are in writing;

(B) Specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition can be satisfied; **and**

(C) Have been implemented, including by taking reasonable steps to ensure that its workforce members and its agents understand and consistently apply the policies and procedures; **or**

(ii) Has been documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and

Exception: Promoting the Privacy of Electronic Health Information

(2) If the precondition relies on the provision of consent or authorization from an individual, the actor:

(i) Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and

(ii) Did not improperly encourage or induce the individual to not provide the consent or authorization.

(3) The actor's practice is—

(i) Tailored to the specific privacy risk or interest being addressed; and

(ii) Implemented in a consistent and non-discriminatory manner.

(c) Health IT developer of certified health IT not covered by HIPAA. If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule when engaging in a practice that promotes the privacy interests of an individual, the actor may choose not to provide access, exchange, or use of electronic health information provided that the actor's practice—

(1) Complies with applicable state or federal privacy laws;

(2) Implements a process that is described in the actor's organizational privacy policy;

(3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service;

(4) Is tailored to the specific privacy risk or interest being addressed; and

(5) Is implemented in a consistent and non-discriminatory manner.

(d) Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3). If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3).

(e) Respecting an individual's request not to share information. In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if—

(1) The individual requests that the actor not provide such access, exchange, or use;

(2) Such request is initiated by the individual without any improper encouragement or inducement by the actor;

(3) The actor or its agent documents the request within a reasonable time period; and

(4) The actor's practice is implemented in a consistent and non-discriminatory manner.

Protecting Privacy: Recommendations

Exception: Promoting the Security of Electronic Health Information

- An actor may implement measures to promote the security of EHI
  - The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI
  - The practice must be tailored to specific security risks and must be implemented in a consistent and non-discriminatory manner
  - The practice must implement an organizational security policy that meets certain requirements or must be based on an individualized determination regarding the risk and response in each case

Are non-HIPAA entities sufficiently addressed?
Organizational policies (some could be information blocking practice; others could enable exception)

Exception: Promoting the Security of Electronic Health Information

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; **and**

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to the electronic health information; **and**

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

Protecting Security: Recommendations

Definitions

Interoperability Defined §170.102

Interoperability is, with respect to health information technology, such health information technology that –

(i) Enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;

(ii) Allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; and

(iii) Does not constitute information blocking as defined in § 171.103 of this subchapter.

Information Blocking Defined: 21st Century Cures

SEC. 3022. INFORMATION BLOCKING. ‘‘(a) DEFINITION.— ‘‘(1) IN GENERAL.—In this section, the term ‘information blocking’ means a practice that— ‘‘(A) except as required by law or specified by the Secretary pursuant to rulemaking under paragraph (3), is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and ‘‘(B)(i) if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or ‘‘(ii) if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

(2) PRACTICES DESCRIBED.—The information blocking practices described in paragraph (1) may include— ‘‘(A) practices that restrict authorized access, exchange, or use under applicable State or Federal law of such information for *treatment and other permitted purposes* under such applicable law, including transitions between certified health information technologies; ‘‘(B) implementing health information technology in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information; and ‘‘(C) implementing health information technology in ways that are likely to— ‘‘(i) restrict the access, exchange, or use of electronic health information with respect to exporting complete information sets or in transitioning between health information technology systems; or ‘‘(ii) lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health information technology.

(3) RULEMAKING.—The Secretary, through rulemaking, shall identify reasonable and necessary activities that do not constitute information blocking for purposes of paragraph (1).

Information Blocking Defined

- 21st Century Cures: summary definition
  - *A practice by a health care provider, health IT developer, health information exchange, or health information network that, except as required by law or specified by the Secretary as a reasonable and necessary activity, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information*
- ONC follows Cures, taking a very broad view of the definition and mitigating with "reasonable and necessary" exceptions
- The Information Blocking provisions (and most new Conditions of Certification) are implemented on the *effective date* of the Final Rule: two month after publication
  - Other proposed rule provisions have somewhat later dates, for example new API certification criteria take effect 24 months after the effective date (development and provider implementation completed)

Information Blocking Defined: ONC Proposed Rule

§ 171.103 Information blocking.

Information blocking means a practice that—

(a) Except as required by law or covered by an exception set forth in subpart B of this part, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and

(b) If conducted by a health information technology developer, health information exchange, or health information network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or

(c) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Information Blocking: Key Definitions §171.102

- *Access:* the ability or means necessary to make EHI available for use, including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained
- *Exchange:* the ability for electronic health information to be transmitted securely and efficiently between and among different technologies, systems, platforms, or networks in a manner that allows the information to be accessed and used
- *Use:* the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose

Interoperability Element §171.102

1. Any functional element of a health information technology, whether hardware or software, that could be used to access, exchange, or use electronic health information for any purpose, including information transmitted by or maintained in disparate media, information systems, health information exchanges, or health information networks.
2. Any technical information that describes the functional elements of technology (such as a standard, specification, protocol, data model, or schema) and that a person of ordinary skill in the art may require to use the functional elements of the technology, including for the purpose of developing compatible technologies that incorporate or use the functional elements.
3. Any technology or service that may be required to enable the use of a compatible technology in production environments, including but not limited to any system resource, technical infrastructure, or health information exchange or health information network element.
4. Any license, right, or privilege that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.
5. Any other means by which EHI may be accessed, exchanged, or used

Note: Interoperability element is a key concept of API and Information Blocking provisions, for example relative to licensing

Electronic Health Information Defined §171.102

- Electronic protected health information (defined in HIPAA), and any other information that:
  - Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
  - Is transmitted by or maintained in electronic media (defined in 45 CFR 160.103) that;
  - Relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- Not limited to information created or received by a provider
- Does not include de-identified health information per 45 CFR 164.514(b)
- Could include price information but ONC has RFI on including price information within EHI with regard to information blocking

Definitions: Recommendations

- Provide suggestions in chat and offline

ONC Examples of Interoperability Practices

Practices: ONC Examples

1. Formal restrictions through contract or license terms, EHI access policies, organizational policies and procedures, or other instruments or documents that relate to EHI or health IT.
2. Exercising IP rights or other rights.
3. Health system policy requiring consent to exchange EHI for treatment even though not required by law.
4. EHR developer refuses to share technical information needed to export data.
5. HIN restriction on end-user sharing EHI with non-HIN members.
6. Health system citing HIPAA as a reason that it cannot share EHI when that it not the case.
7. EHR vendor only provides EHI in PDF format upon termination of an agreement with a customer.
8. An EHR developer sues to prevent a clinical data registry from providing interfaces to physicians who use the developer's EHR technology and wish to submit EHI to the registry. The EHR developer claims that the registry is infringing the developer's copyright in its database because the interface incorporates data mapping that references the table headings and rows of the EHR database in which the EHI is stored.
9. A health IT developer of certified health IT refuses to license interoperability elements that are reasonably necessary for the developer's customers, their IT contractors, and other health IT developers to develop and deploy software that will work with the certified health IT.
10. An EHR developer ostensibly allows third-party developers to deploy apps that are interoperable with its EHR system. However, as a condition of doing so, the third-party developers must provide their source code and grant the EHR developer the right to use it for its own purposes—terms that almost no developer would willingly accept.
11. Disabling or restricting the use of a capability that enables users to share EHI with users of other systems or to provide access to EHI to certain types of persons or for certain purposes that are legally permissible.
12. An actor configures or otherwise implements technology in ways that limit the types of data elements that can be exported or used from the technology.
13. Configuring capabilities in a way that removes important context, structure, or meaning from the EHI, or that makes the data less accurate, complete, or usable for important purposes for which it may be needed.
14. Implementing capabilities in ways that create unnecessary delays or response times, or that otherwise limit the timeliness of EHI accessed or exchanged.
15. An actor deploys technological measures that limit or restrict the ability to reverse engineer the functional aspects of technology in order to develop means for extracting and using EHI maintained in the technology.
16. A health system implements locally-hosted EHR technology certified to proposed § 170.315(g)(10) (the health system acts as an API Data Provider as defined by § 170.102). As required by proposed § 170.404(b)(2), the technology developer provides the health system with the capability to automatically publish its production endpoints (i.e., the internet servers that an app must "call" and interact with in order to request and exchange patient data). The
17. health system chooses not to enable this capability, however, and provides the production endpoint information only to apps it specifically approves. This prevents other applications—and patients that use them—from accessing data that should be made readily accessible via standardized APIs.
18. A hospital directs its EHR developer to configure its technology so that users cannot easily send electronic patient referrals and associated EHI to unaffiliated providers, even when the user knows the Direct address and/or identity (i.e., National Provider Identifier) of the unaffiliated provider.
19. An EHR developer that prevents (such as by way of imposing exorbitant fees unrelated to the developer's costs, or by some technological means) a third-party clinical decision support (CDS) app from writing EHI to the records maintained by the EHR developer on behalf of a health care provider (despite the provider authorizing the third-party app developer's use of EHI) because the EHR developer: (1) offers a competing CDS software to the third-party app; and (2) includes functionality (e.g., APIs) in its health IT that would provide the third party with the technical capability to modify those records as desired by the health care provider.
20. Although an EHR developer's patient portal offers the capability for patients to directly transmit or request for direct transmission of their EHI to a third party, the developer's customers (e.g., health care providers) choose not to enable this capability.
21. A health care provider has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient's health care provider but takes several days to respond.

Practices: ONC Examples

22. A health IT developer of certified health IT refuses to license an API's interoperability elements, to grant the rights necessary to commercially distribute applications that use the API's interoperability elements, or to provide the related services necessary to enable the use of such applications in production environments.
23. An EHR developer of certified health IT requires third-party applications to be "vetted" for security before use but does not promptly conduct the vetting or conducts the vetting in a discriminatory or exclusionary manner.
24. A health IT developer of certified health IT refuses to license interoperability elements that other software applications require to efficiently access, exchange, and use EHI maintained in the developer's technology.
25. An EHR developer of certified health IT maintains an "app store" through which other developers can have "apps" listed that run natively on the EHR developer's platform. However, if an app "competes" with the EHR developer's apps or apps it plans to develop, the developer *requires* that the app developer grant the developer the right to use the app's source code.
26. A health care provider engages a systems integrator to develop an interface engine. However, the provider's license agreement with its EHR developer prohibits it from disclosing technical documentation that the systems integrator needs to perform the work. The EHR developer states that it will only permit the systems integrator to access the documentation if all of its employees sign a broad non-compete agreement that would effectively bar them from working for any other health IT companies.
27. An EHR developer of certified health IT maintains an "app store" through which other developers can have "apps" listed that run natively on the EHR developer's platform. The EHR developer charges app developers a substantial fee for this service unless an app developer agrees not to deploy the app in any other EHR developers' app stores.
28. A hospital is working with several health IT developers to develop an application that will enable ambulatory providers who use different EHR systems to access and update patient data in the hospital's EHR system from within their ambulatory EHR workflows. The inpatient EHR developer, being a health IT developer of certified health IT, pressures the hospital to abandon this project, stating that if it does not it will no longer receive the latest updates and features for its inpatient EHR system.
29. A health IT developer of certified health IT discourages customers from procuring data integration capabilities from a third-party developer, claiming that it will be providing such capabilities free of charge in the next release of its product. In reality, the capabilities it is developing are more limited in scope and are still 12-18 months from being production-ready.
30. A health system insists that local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and facilities. The health system threatens to revoke admitting privileges for physicians that do not comply.
31. An HIN charges additional fees, requires more stringent testing or certification requirements, or imposes additional terms for participants that are competitors, are potential competitors, or may use EHI obtained via the HIN in a way that facilitates competition with the HIN.
32. A health care provider imposes one set of fees and terms to establish interfaces or data sharing arrangements with several registries and exchanges but offers another costlier or significantly onerous set of terms to establish substantially similar interfaces and arrangements with an HIE or HIN that is used primarily by health plans that purchase health care services from the provider at negotiated reduced rates.
33. A health IT developer of certified health IT charges customers fees, throttles speeds, or limits the number of records they can export when exchanging EHI with a regional HIE that supports exchange among users of competing health IT products but does not impose like fees or limitations when its customers exchange EHI with enterprise HIEs that primarily serve users of the developer's own technology.
34. As a condition of disclosing interoperability elements to third-party developers, an EHR developer requires third-party developers to enter into business associate agreements with all of the EHR developer's covered entity customers, even if the work being done is not for the benefit of the covered entities.
35. A health IT developer of certified health IT takes significantly longer to provide or update interfaces that facilitate the exchange of EHI with users of competing technologies or services.
36. Certain practices that artificially increase the cost and expense associated with accessing, exchanging, and using EHI will implicate the information blocking provision. 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.
37. An EHR developer of certified health IT charges customers a fee to provide interfaces, connections, data export, data conversion or migration, or other interoperability services, where the amount of the fee exceeds the actual costs that the developer reasonably incurred to provide the services to the particular customer(s).
38. An EHR developer of certified health IT charges a fee to perform an export using the EHI export capability proposed in § 170.315(b)(10) for the purposes of switching health IT systems or to provide patients access to EHI.

Practices: ONC Examples

39. An EHR developer of certified health IT charges more to export or use EHI in certain situations or for certain purposes, such as when a customer is transitioning to a competing technology or attempting to export data for use with a HIE, third-party application, or other technology or service that competes with the revenue opportunities associated with the EHR developer's own suite of products and services.
40. An EHR developer of certified health IT interposes itself between a customer and a third-party developer, insisting that the developer pay a licensing fee, royalty, or other payment in exchange for permission to access the EHR system or related documentation, where the fee is not reasonably necessary to cover any additional costs the EHR developer incurs from the third-party developer's activities.
41. An analytics company provides services to the customers of an EHR developer of certified health IT, including de-identifying customer EHI and combining it with other data to identify areas for quality improvement. The EHR developer insists on a revenue sharing arrangement whereby it would receive a percentage of the revenue generated from these activities in return for facilitating access to its customers' EHI, which turns out to be disadvantageous to customers. The revenue the EHR developer would receive exceeds its reasonable costs of facilitating the access to EHI.
42. 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.
43. 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.

Certification

Attestations §170.406

- Condition of Certification: A health IT developer must provide an attestation, as applicable, to compliance with Conditions and Maintenance of Certification, except for "EHR reporting”
- Maintenance of Certification: Health IT developers must attest every six months

Conditions of Certification: Information Blocking §170.402

- As a *Condition of Certification* and to maintain such certification, a health IT developer must not take any action that constitutes information blocking as defined in section 4004 of the Cures Act
  - In some cases, these go beyond specific certification criteria, for example, information blocking focuses on EHI rather than the USCDI and *use* includes *write* and extends beyond the proposed new API certification criteria
  - There are specific fee and transparency requirements as part of the API Condition of Certification
- This provision is subject to the 7 proposed exceptions to information blocking definition, which define reasonable and necessary activities
- No Maintenance of Certification beyond ongoing compliance
- Must also provide assurances
- This provision and the other new Conditions and Maintenance of Certification are implemented as of the effective date of a final rule

Application at company level. Access beyond USCDI? Unintended consequences?

Conditions of Certification: Assurances §170.402

- A health IT developer must provide assurances to the Secretary (unless for reasonable and necessary activities identified by the Secretary) that it will not take any action that constitutes information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI.

Do assurances add value or increase risks?

Conditions of Certification: APIs §170.404

- Apply to:
  - *API Technology Suppliers (Suppliers)* with health IT certified to any API-focused certification criteria
  - *API Data Provider:* Health care organization that deploys the API technology
  - *API User*: Persons and entities that use or create software applications that interact with API technology

- *Transparency*: ONC proposes that Suppliers make business & technical documentation necessary to interact with their APIs freely and publicly accessible
- *Permitted fees*: ONC has proposed to adopt detailed conditions that govern fees Suppliers could charge and to whom fees could be charged – detailed record keeping
- *Pro-competitive*: ONC proposes that Suppliers would have to comply with requirements to promote an open and competitive marketplace

How do API requirements interact with information blocking restrictions? Any conflicts?

APIs §170.404

Conditions of Certification

- Requires health IT developers to publish APIs that allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law
- Through the APIs, a developer must also provide access to all data elements (i.e., the USCDI) of a patient's EHR to the extent permissible under applicable privacy laws
- Note: EHI is broader than "all data: as USCDI
- An API Technology Supplier must make business and technical documentation necessary to interact with their APIs in production freely and publicly accessible
- All fees related to API technology, not otherwise permitted by this section, are prohibited from being imposed by an API technology Supplier.
- API Technology Suppliers must grant API Data Providers (i.e., health care providers who purchase or license API technology) the sole authority and autonomy to permit API Users to interact with the API technology

Maintenance of Certification

- An API Technology Supplier must register and enable all applications for production use within one business day of completing its verification of an applications developer's authenticity
- A Supplier must support publication of "Service Base URLs" (i.e., FHIR® server endpoints) for all of its customers, regardless of those that are centrally managed by the Supplier or locally deployed by an API Data Provider, and make such information publicly available at no charge

API: Fees §170.404

API fees. Any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:

(*1*) The persons or classes of persons to whom the fee applies;

(*2*) The circumstances in which the fee applies; **and**

(*3*) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

Permitted fees conditions. (i) *General conditions*. (A) All fees related to API technology not otherwise permitted by this section are prohibited from being imposed by an API Technology Supplier.

(B) For all permitted fees, an API Technology Supplier must:

(*1*) Ensure that fees are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(*2*) Ensure that fees imposed on API Data Providers are reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting API technology to, or at the request of, the API Data Provider to whom the fee is charged.

(3) Ensure that the costs of supplying and, if applicable, supporting the API technology upon which the fee is based are reasonably allocated among all customers to whom the API technology is supplied, or for whom the API technology is supported.

(4) Ensure that fees are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier.

(ii) Permitted fee – Development, deployment, and upgrades. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider.

(iii) Permitted fee – Supporting API uses for purposes other than patient access. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the incremental costs reasonably incurred by the API Technology Supplier to support the use of API technology deployed by or on behalf of the API Data Provider. This permitted fee does not include:

(A) Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information;

(B) Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or

(C) Opportunity costs, except for the reasonable forward-looking cost of capital.

(iv) Permitted fee – Value-added services. An API Technology Supplier is permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software.

(v) Record-keeping requirements. An API Technology Supplier must keep for inspection detailed records of any fees charged with respect to the API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

API: Read and Write

Certification

- *This proposed certification criterion would only require mandatory support for "read" access for both identified services, though we envision a future version of this certification criterion that could include specific "write" conformance requirements (for example, to aid decision support) once FHIR-based APIs are widely adopted.*

Information Blocking

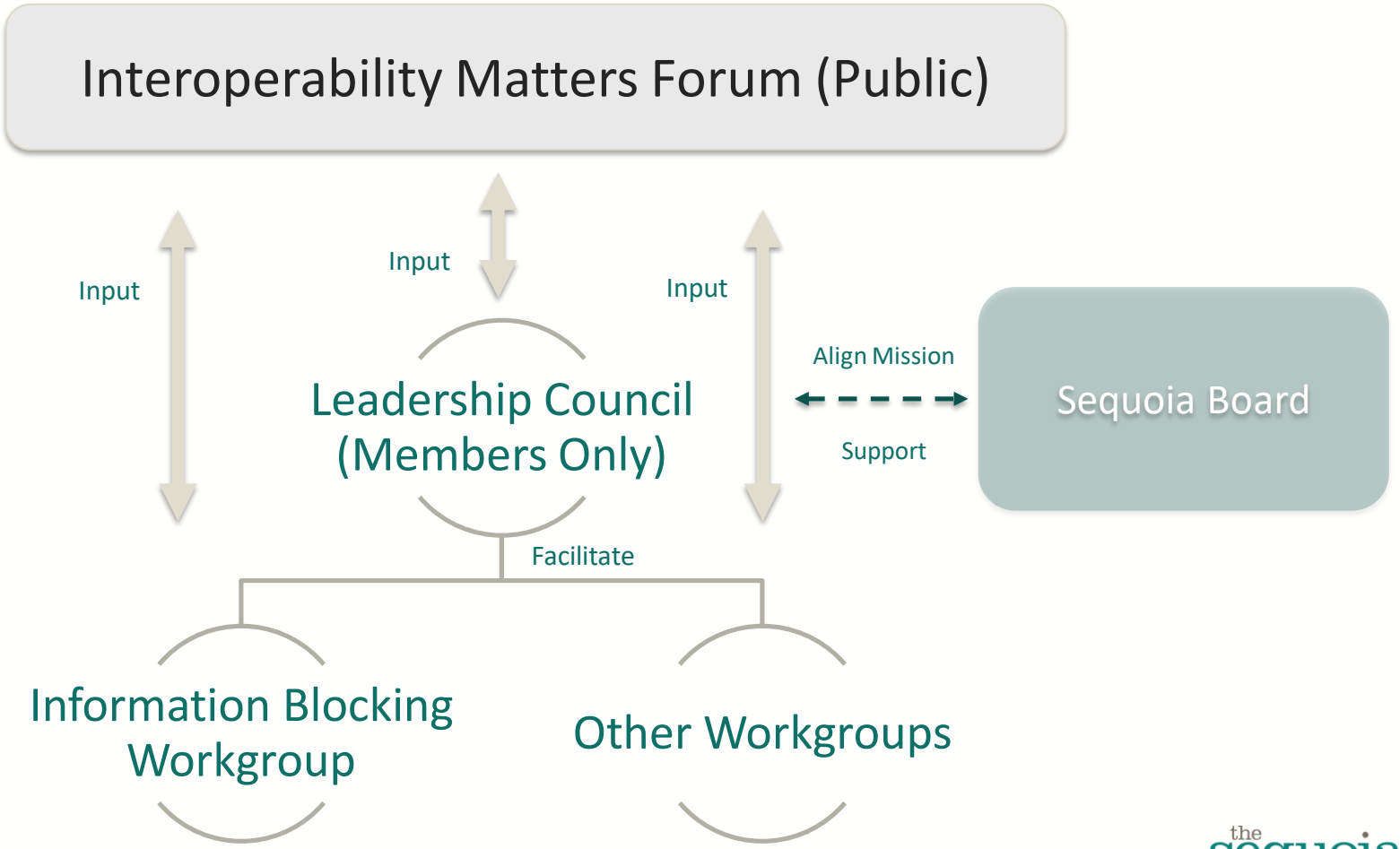
- *For example, the definition of "use" includes the ability to read, write, modify, manipulate, or apply EHI to accomplish a desired outcome or to achieve a desired purpose, while "access" is defined as the ability or means necessary to make EHI available for use. As such, interference with "access" would include, for example, an interference that prevented a health care provider from writing EHI to its health IT or from modifying EHI stored in health IT, whether by the provider itself or by, or via, a third-party app.*

Interoperability Matters

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 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

Materials for Remaining Workgroup Meetings

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

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

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*

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

Note: Cures statutory provisions are out of scope for recommended changes other than for information and as a point of reference

Key Concepts for Workgroup Review

Actors

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

Blocking Practices

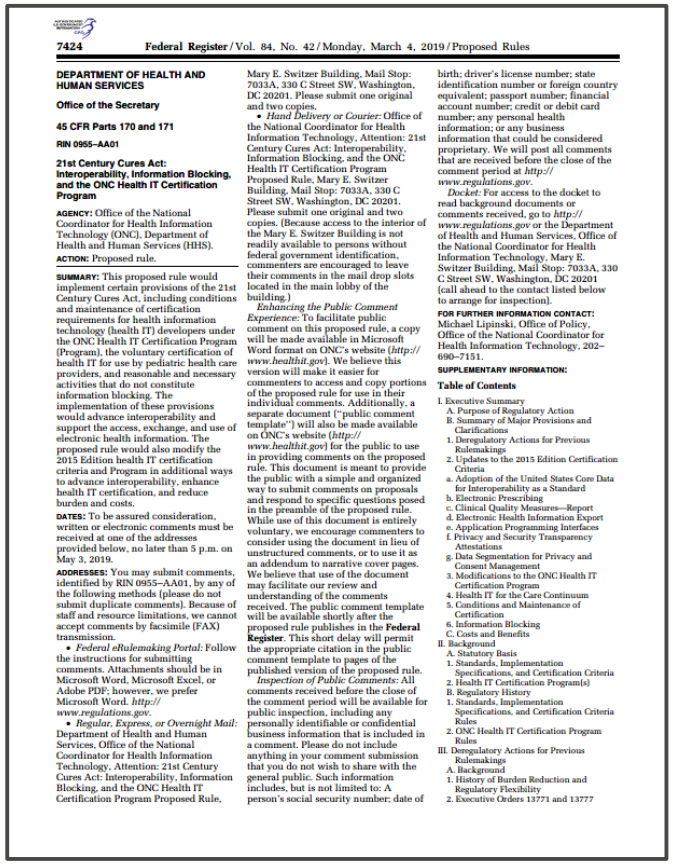
- *Restrictions on access, exchange, or use* of EHI through formal means (e.g., contractual restrictions) or informal means (e.g., ignoring requests to share EHI)
- *Limiting or restricting the interoperability of health IT* (e.g., disabling a capability that allows users to share EHI with users of other 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

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:

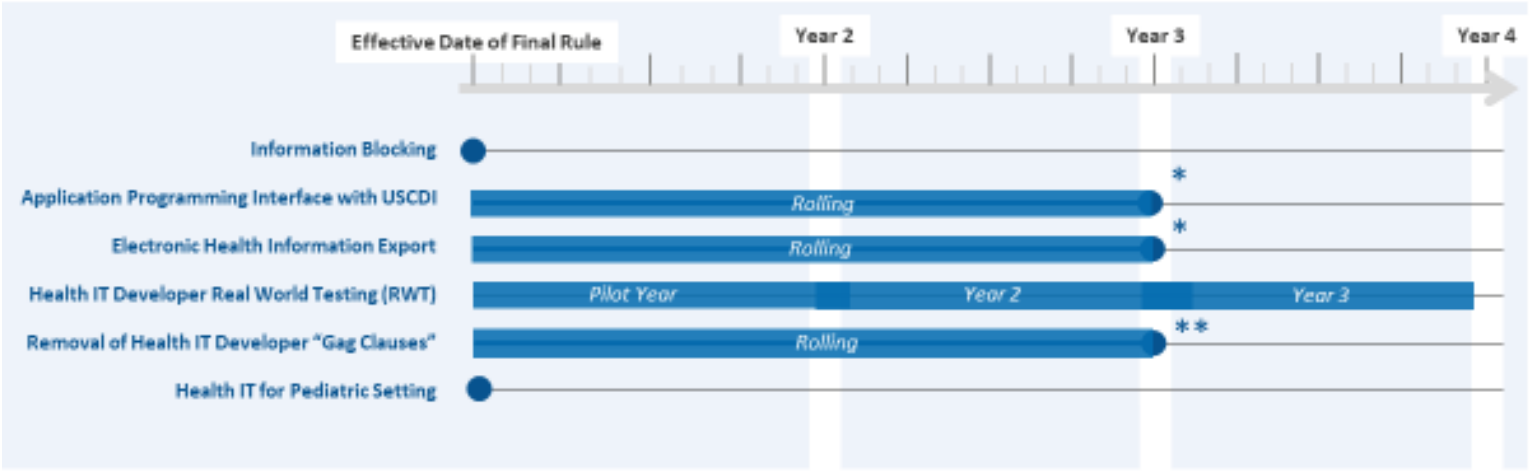
Table of Contents

Workgroup Meeting #4

- Review Draft Workgroup Report (circulated one week before meeting)

21st Century Cures Act NPRM – Regulatory Implementation Milestones

21ST CENTURY CURES ACT NPRM – REGULATORY IMPLEMENTATION MILESTONES



*Last day for health IT developers to implement for customers (health care providers)
**Last day to remove "gag clauses" from health IT contracts

The Office of the National Coordinator for Health Information Technology

Interoperability Matters

https://sequoiaproject.org/interoperability-matters/