Information Blocking Workgroup Meeting #4

Interoperability Matters

4/15/2019
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

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

*Invited
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—including 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 policies 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 opportunist 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 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](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 be 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 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 considered 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.
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
Public Comments
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
• Next Public Advisory Forum on May 23rd 1 p.m. ET
• Thank you all!
Background
Key Milestones

- Proposed Rule Published
  March 4, 2019

- Public Advisory Forum #1
  March 19, 2019

- Leadership Council Mtg #1
  March 29, 2019

- Public Advisory Forum #2
  April 5, 2019

- Leadership Council Mtg #2
  April 22, 2019

- Comments due to ONC
  May 3, 2019

- Workgroup Mtg #1
  March 14, 2019

- Public Launch
  March 14, 2019

- Workgroup Mtg #2
  March 25, 2019

- Workgroup Mtg #3
  April 3, 2019

- Workgroup Mtg #4 – Public call regarding draft report
  April 15, 2019

- Sequoia Board Meeting
  April 26, 2019

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

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