Information Blocking Workgroup: Meeting 1

Interoperability Matters

3/14/2019

Agenda

- Welcome and Introductions
- Interoperability Matters
- Information Blocking Work Group
- Workplan
- Overview of Scope
- Discussion

Information Blocking Workgroup: Members and Staff

- Workgroup Members
  - David Camitta, MD, Dignity Health, Co-Chair
  - Paul Uhrig, Surescripts, Co-Chair
  - Workgroup Representatives

- Staff Support and Facilitators
  - Steve Gravely
  - Shawna Hembree
  - Mark Segal
  - Mariann Yeager

Workgroup Representatives

Associations and Orgs - health IT community
- Lauren Riplinger, AHIMA
- Matt Reid, AMA
- Tom Leary / Mari Greenberger, HIMSS*

Consumers
- Ryan Howells, CARIN Alliance

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

Health Information Networks and Service Providers
- Dave Cassel, Carequality
- Chuck Christian, IHIE
- Brian Ahier, Medicity / Health Catalyst
- Paul Uhrig, Surescripts, Co-Chair

Healthcare Provider
- David Camitta, Dignity, Co-Chair
- Wendy Angelo, Indiana Regional Med. Center*
- Eric Liederman, Kaiser

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

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

Public Health
- John Loonsk, CGI

Vendors
- Josh Mast, Cerner
- Cherie Holmes-Henry, EHRA / NEXTGEN
- Rob Klootwyk, Epic
- Aashima Gupta, Google*

Informatics
- Doug Fridsma, AMIA

Safety net providers / service provider
- Jennifer Stoll, OCHIN

Release of Information Company
- Rita Bowen, MROCorp

**Invited*

Interoperability Matters Background

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 Process

Sequoia Board

- Approves priorities, charters, resources
- Assures alignment with Sequoia mission
- Board Committee supports Cooperative, in consultation with Leadership Council
- Approves official Sequoia policy positions

Leadership Council

- Facilitates Cooperative
- Recommends priorities to Board
- Charters Workgroups, with Board approval
- Oversees Workgroup process
- Assures advisory Forum input
- Presents findings, recommendations, work products to Board

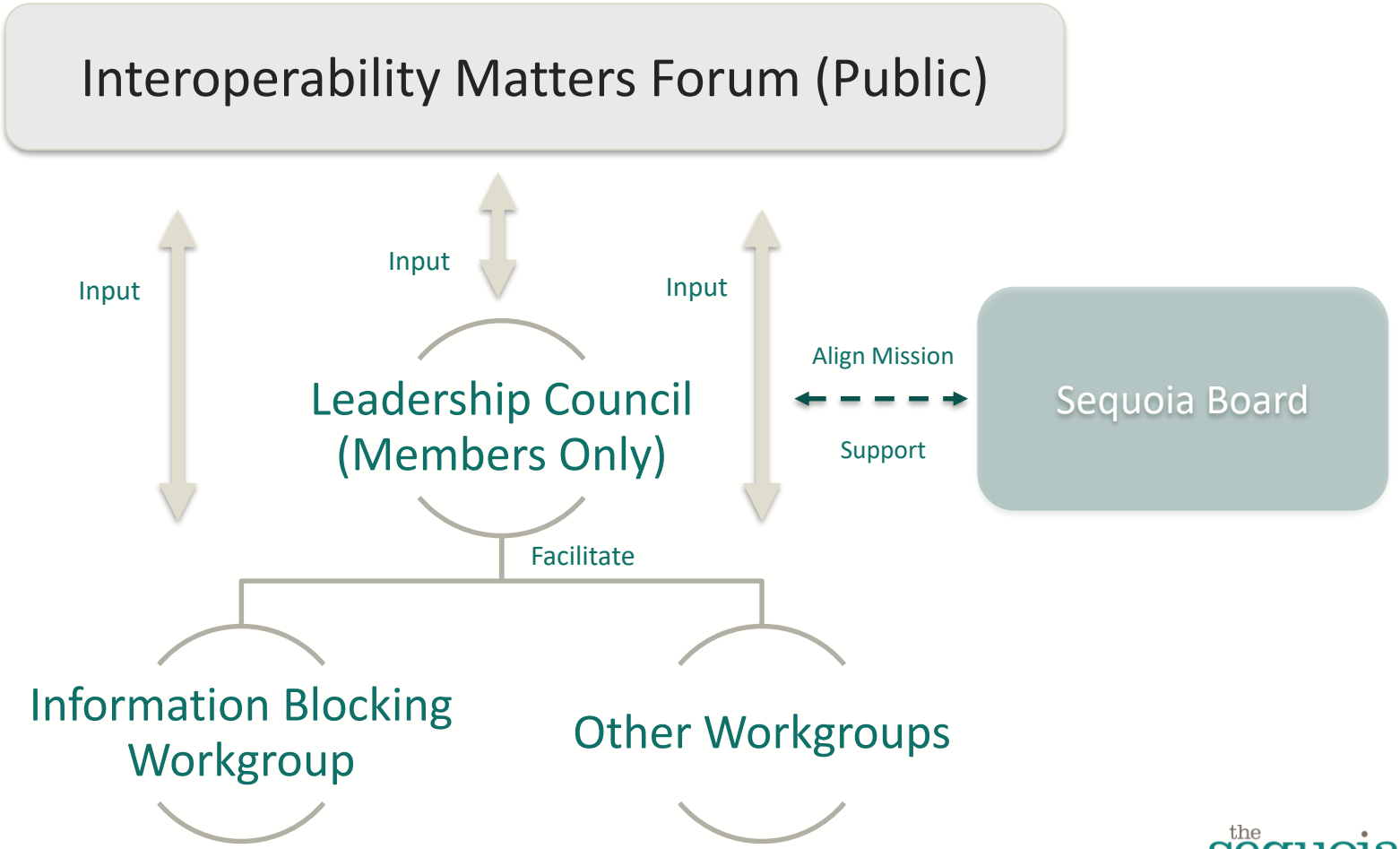
Work Group

- Conducts detailed work
- Drafts findings, recommendations, work products
- Enlists input from advisory Forum
- Presents its work to Leadership Council for acceptance

Interoperability Matters Forum

- Convened public forum
- Provides input to Leadership Council and Workgroups
- Reflects diverse perspectives
- Is informed of progress
- Support Affinity Groups if consensus or input sought from particular perspective

Interoperability Matters Structure



Leadership Council Purpose and Process

- Purpose:
  - Lead the Interoperability Matters Cooperative for the benefit of Sequoia and the interoperability community
- Role:
  - Facilitate open, inclusive Cooperative process, including public-facing and workgroup efforts
  - Aim for consensus but accommodate and reflect varying community perspectives
  - Serve as liaison to Sequoia board

Leadership Council (Members Only)

- Structure: Members-Only (Voting and Non-Voting)
- Role
  - Facilitates the Cooperative's work
  - Consults with Sequoia Board Committee and Interoperability Matters Forum on priorities
  - Develops workgroup charters, subject to board approval
  - Coordinates workgroup and advisory Forum efforts
    - Recruits workgroup members
    - Tracks workgroup progress and guides effort
    - Assures appropriate input from advisory Forum
  - Provides substantive input to Board Committee and workgroups
    - Shares guidance, observations and other perspectives
    - Vets work group deliverables prior to submission to Board Committee
    - Considers advisory Forum input
  - Serves as liaison to Sequoia Board Committee
    - Presents recommended priorities
    - Reports status and progress
    - Presents deliverables and recommendations

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

Prioritization Process

- Proposals for a project may come from any source
- Proposals are submitted to the Leadership Council for consideration
- Leadership Council vets and narrows down proposed projects
- Leadership Council facilitates input from Interoperability Matters Forum
- Leadership Council finalizes priorities in consultation with Sequoia Board
- Sequoia Board assures alignment with Sequoia mission
- Sequoia Board approves resources to support the proposed projects

Work Product / Adoption Process

Example: Coordinated Implementation Plan (e.g. C-CDA,USCDI Evolution)

- Leadership Council charters workgroup in consultation with Board Committee
- Leadership Council recruits workgroup members
- Workgroup facilitates work (e.g. deployment timeline, versioning, etc.), with Sequoia facilitator and staff support
- Workgroup co-chairs brief Leadership Council regarding its work
- Leadership Council co-chairs brief Board Committee regarding workgroup
- Workgroup shares progress and enlists input from Interoperability Matters Forum
- Interoperability Matters Forum shares perspectives in public meeting
- Workgroup considers input and recommends rollout plan
- Sequoia Board approves official Sequoia positions, findings and/or recommendations to policymakers

Public Policy/Comment Process

Information Blocking Workgroup

- Leadership Council charters workgroup in consultation with Sequoia board
- Sequoia staff / facilitators prepare materials for facilitated Workgroup discussions
- Workgroup Co-Chairs facilitate workgroup calls with staff and facilitator support
- Interoperability Matters Forum consulted regarding specific matters
  - Iterative basis as timeline permits
  - Focus on key questions, assumptions, interpretations, policy positions
  - Gauge where consensus and enlists diverse perspectives
- Workgroup convenes to:
  - Draft findings and recommendations based upon input
  - Include additional opportunities for public comment in Workgroup calls
  - Consult with Leadership Council
  - Finalize findings and recommendations
  - Present to Leadership Council for approval
- Leadership Council shares approved findings / recommendations with Board Committee
- Board Committee advises Sequoia Board (e.g. share, endorse, approve)

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

Composition

- Public call issued to serve on forum, regardless of Sequoia affiliation
- Open to all stakeholders, with the following represented at minimum:
  - Associations and organizations representing health IT community
  - Federal government representatives
  - Health information networks and service providers
  - Healthcare provider organizations, physicians and other clinicians
  - Individuals
  - Payers
  - Public Health
  - Subject matter experts (legal, privacy, information sharing policy, technology, standards)
  - Vendors (e.g. EHR, health IT to connect to EHRs, 3rd party integrators, consumer apps)
- Emphasis on experience applying information sharing policies and rules within their respective organizations

Leadership and Staffing

- Two co-chairs lead the Workgroup
  - Appointed by the Sequoia Board, in consultation with Leadership Council
  - Have subject matter expertise, leadership and facilitation skills
  - Represent different stakeholder groups
  - May engage other stakeholders and SMEs to support work
  - Establish subgroups as necessary, with reports to Workgroup
- Sequoia staff and facilitators support Workgroup
  - Conduct analysis
  - Prepare discussion materials
  - Facilitate discussion of specific matters
  - Prepare deliverables

Workgroup Member Responsibilities

- Maintain personal involvement in Workgroup meetings
- Respect any confidential discussions held in the Workgroup
- Represent necessary expertise to contribute to Workgroup deliverables
- Enlist feedback from the constituents represented
- Balance personal perspectives with those of the constituency represented
- Gain input from and communicate to constituency
- Accept occasional assignments tasks between Workgroup meetings

Workgroup Process

- Open, inclusive, consensus-based process, with ability to move forward and capture range of views expressed
- Facilitate formal process (e.g. published meeting agenda, meeting notes with roll, outcomes, Workgroup roster, documented decisions, etc.)
- Accommodate and reflect varying community perspectives and needs
- Focus on priority use cases consistent with Sequoia's mission and Interoperability Matters
- Remain vendor, provider, and technology neutral

Consensus and Decision-Making

- Aim for consensus, where possible
- With or without consensus
  - Assure diverse stakeholder views heard
  - Identify areas of agreement
  - Capture diverse perspectives
  - Consider recommendations for further study to move towards consensus
  - Document the range of positions

Phased Work

- Phase I: Review and provide perspectives on information blocking provisions of ONC proposed rule
- Phase II: Self-identify additional work items
  - Guidance and development of consensus points on practices relevant to information blocking laws and regulations
  - Input to federal government on implementation of information blocking laws and regulations
  - Provide subject matter expertise to support development and maintenance of information blocking-related materials to support the community.
  - Use webinars, wikis, online surveys and other mechanisms to gain community feedback
  - Conclude at discretion of Leadership Council, in consultation with Sequoia Board

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*) 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

Timetable and Schedule

- Proposed Rule Published — March 4, 2019
- Initial Workgroup meeting — March 14, 2019
- Workgroup meetings
  - Meeting #2 — March 25, 12:30-1:30 EDT
  - Meeting #3 — April 3, 1:00-2:00 EDT
  - Meeting #4 — April 15, 12:00-1:00 EDT
- Public Advisory Forums
  - Meeting #1 — March 19, 3:00-4:00 EDT
  - Meeting #2 — April 5, 2019
  - Meeting #3 — April 15
    **Public call regarding Draft Report*
- Feedback to Leadership Council
  - Meeting #1 — March 29, 2019
  - Meeting #2 — April 22 or 23, 2019
  - Sequoia Board meeting — April 26
- Comments due to ONC — May 3, 2019

Information Blocking Proposed Rule: Overview and Workgroup Scope

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* 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: 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: 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

Information Blocking Unpacked

- *Practice(s)*—The focus is on what an actor does not what it meant to do. The actual conduct of an actor will be the evidence of information blocking.
- *Prevent or materially discourage*—The government does not have to show that an actor actually prevented access, exchange or use of EHI; it is enough to violate the statute and regulation if an actor's *practices discourage* access, exchange or use of EHI.
- *Access, exchange or use*—The scope of prohibited activities goes well beyond exchange of information but extends to access and use of information.
- *Knows, should know* —Actors cannot "stick their heads in the sand" and claim that they did not realize that their practices would prevent or materially discourage the access, exchange or use of EHI; an actor is liable if they should have known that their practices would prevent or materially discourage access, exchange or use of EHI.
- *Likely to interfere—Actual interference* is not required to violate the law or proposed regulation; practices that have a likelihood of interfering are prohibited; this is much broader than a focus on actual interference.

The definition of information blocking is so broad that almost anything that impedes information flow in any manner could be considered a violation.

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

Proposed 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*

Workgroup Meeting #2

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

Workgroup Meeting #3

Exceptions

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

Other

- ONC RFI: disincentives for providers and price transparency
- Complaint process and enforcement
- Information Blocking elements of Conditions and Maintenance of Certification, including enforcement

Workgroup Meeting #4

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

Additional Background

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: 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 §171.103

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.

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.

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

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

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

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

Information Blocking: Exceptions

- Section 4004 of Cures authorizes HHS Secretary to identify *reasonable and necessary* activities that are not information blocking
- ONC has identified 7 categories of blocking that would be reasonable and necessary, *if certain conditions are met (*45 CFR 171.201–207)
- If actions of an *actor* (health care provider, health IT developer, or health information exchange or network) *satisfy one or more exception*, these *would not be treated as information blocking* and therefore not subject to civil penalties and other disincentives
  - Most exceptions apply to all actors, unless otherwise indicated
- ONC applies Cures definitions or establishes definitions by regulation

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*

Exceptions §171.201

- 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
- The actor has the burden of proving compliance with the exception in the event of an investigation

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*

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.

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*

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.

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

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.

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 *that exceeds 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*

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.

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

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.

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

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.

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

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.

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.*

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

Complaint Process

- 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

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
  - Note, 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
  - Note also that 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 requirements beyond ongoing compliance
- This provision and the other new Conditions and Maintenance of Certification are implemented as of the effective date of a final rule

Conditions of Certification: Information Blocking: 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.*
- *A health IT developer must ensure that its certified health IT conforms to the full scope of the applicable certification criteria*
- *Developers of certified health IT must provide assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes*
- A health IT developer that produces and electronically manages EHI must certify health IT to the 2015 Edition "electronic health information export" certification criterion in § 170.315(b)(10)
  - *Maintenance of Certification*: Must provide all customers with Certified HIT with this functionality within 24 months of final rule effective date or within 12 months of certification for a developer that never previously certified health IT to the 2015 Edition, whichever is longer
- *Maintenance of Certification:* A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:
  - A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or
  - If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.
- ONC is requesting comment as to whether certain health IT developers should be required to participate in the Trusted Exchange Framework and adhere to the Common Agreement
  - Would apply to health IT developers that certify to capabilities used for interoperability (i.e., §§ 170.315(b)(1), (c)(1) and (c)(2), (e)(1), (f), and (g)(9) through (11))

Application Programming Interfaces §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

Conditions of Certification: Application Programming Interfaces §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

Application Programming Interfaces: 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

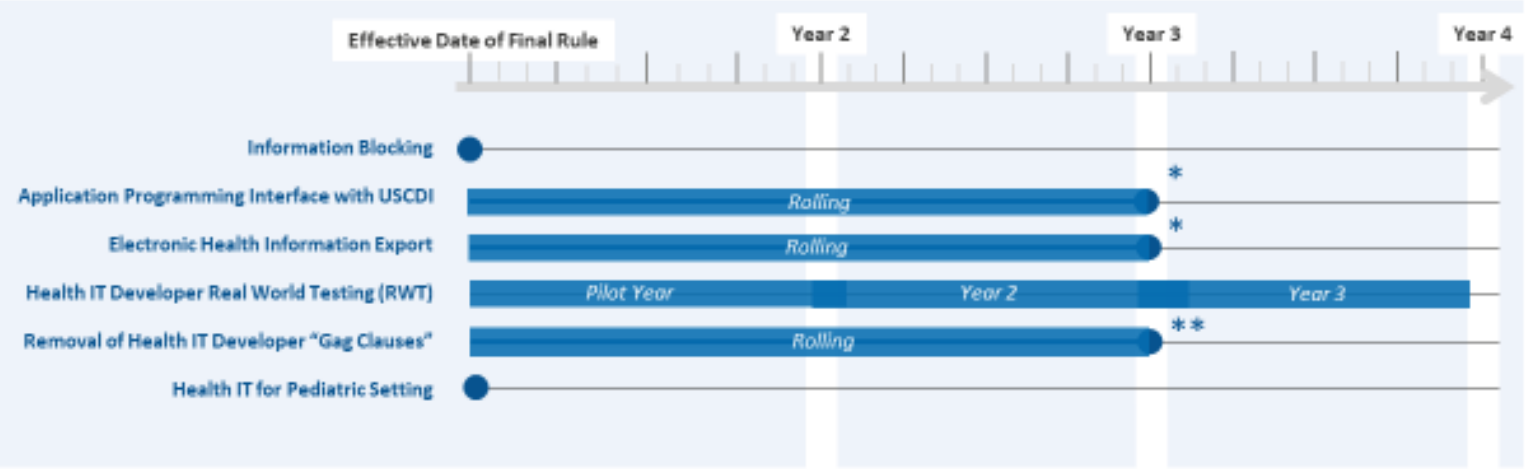
- *For example, the definition of "use" includes the ability to read, write, modify, manipulate, or apply EHI to accomplish a desired outcome or to achieve a desired purpose, while "access" is defined as the ability or means necessary to make EHI available for use. As such, interference with "access" 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.*

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

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