Information Blocking Workgroup Meeting #11

Interoperability Matters

3/20/2020

Workgroup Representatives

Associations and Orgs - health IT community
- Anne Kimbol, HITRUST Alliance
- Mari Greenberger, HIMSS
- Lauren Riplinger, AHIMA
- Scott Stuewe, DirectTrust
- Samantha Burch, AHA

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

Consultant
- Brian Ahier, MITRE Corporation

Federal Government
- Steve Bounds, SSA

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 Providers / Physicians
- David Camitta, CommonSpirit, Co-Chair
- Eric Liederman, Kaiser Permanente
- Matt Reid, AMA
- Mari Savickis, CHIME

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

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

Public Health
- John Loonsk, APHL

Vendors
- Aashima Gupta, Google
- Cherie Holmes-Henry, EHRA/NextGen
- Rob Klootwyk, Epic
- Josh Mast, Cerner
- Vince Vitali, NextGate

Informatics
- Jeff Smith, AMIA

Safety Net Providers / Service Provider
- Jennifer Stoll, OCHIN

Release of Information Company
- Rita Bowen, MROCorp

The Sequoia Project Team

Lindsay Austin, Troutman Sanders Strategies

Steve Gravely, Gravely Group

Shawna Hembree, Program Manager

Mark Segal, Digital Health Policy Advisors

Dawn VanDyke, Director, Marketing Communications

Mariann Yeager, CEO

Agenda

- Welcome and Introductions
- Review of Agenda
- Review ONC Final Rule
- Implementation Planning: Continue from January Call
  - Slides 7 and 8
- Additional Phase 3 Priorities
  - Review from January Call
- Next Steps
- Closing

Information Blocking Workgroup: Purpose

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

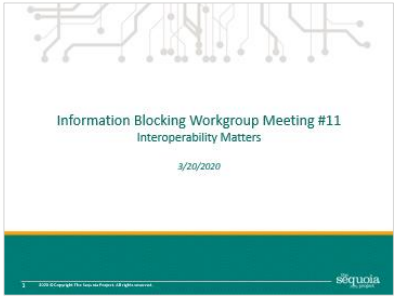
Information Blocking Workgroup: Phase 2/3 Recap

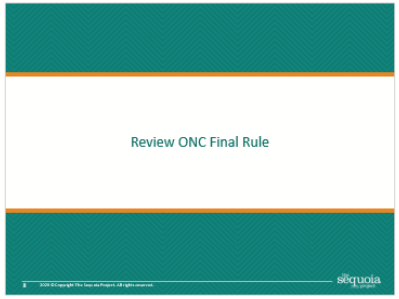
Overall approach: Focus on implementation and compliance implications of ONC proposed rule elements and likely outcomes. Not relitigating comments.

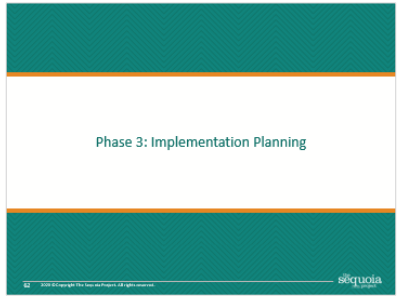
- ✓ Meeting 1 (6/20) Review comments submitted and proposed workplan
- ✓ Meeting 2 (8/2) HIE/HIN and Other Key Definitions
- ✓ Joint Workgroup & Leadership Council (8/21) – In-person and virtual
- ✓ Meeting 3 (9/13) Information Blocking Practices
- ✓ Meeting 4 (10/11) Recovering Costs/RAND Licensing
- ✓ Meeting 5 (11/8) Compliance Plans
- ✓ Meeting 6 (12/13) Compliance Plans (cont.) and Phase 2 Review

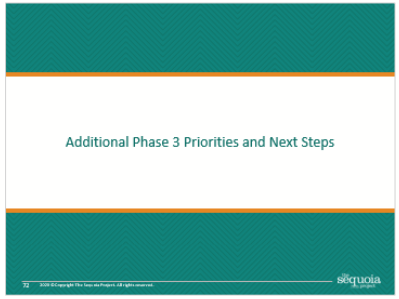
Deliverable Completed: Summary of Phase 2: Guidance to the Community and Implementation Feedback to ONC

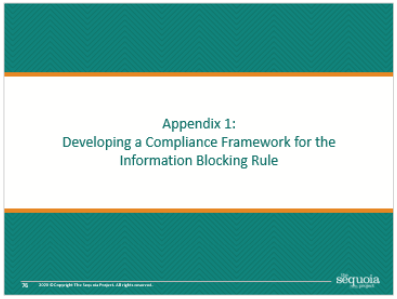
Organization of this Deck

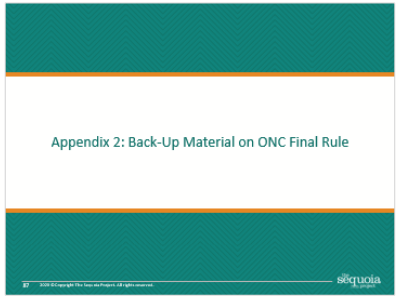


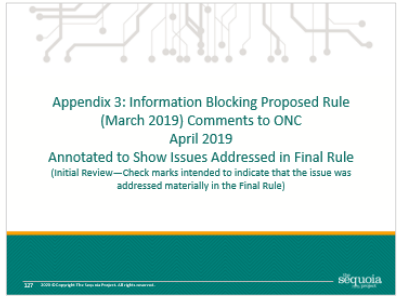


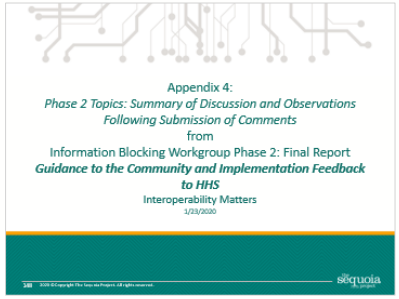












Review ONC Final Rule

21st Century Cures: Information Blocking (Section 4004)

A **practice** that:

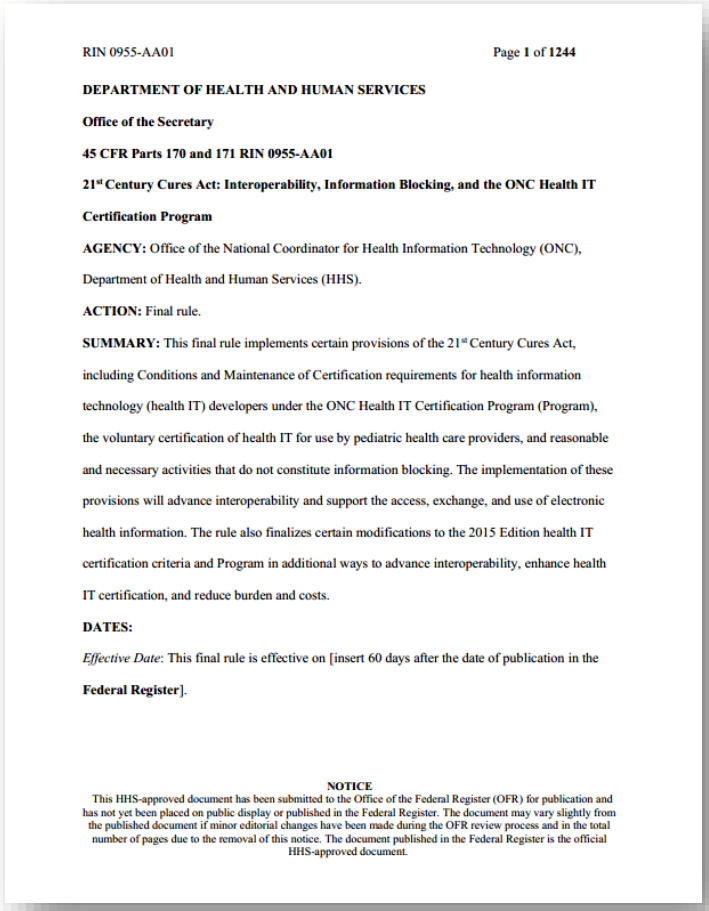
- Except as required by law or specified by the Secretary per ***rulemaking), likely*** to ***interfere with, prevent, or materially discourage access, exchange, or use*** of ***electronic health information*** (EHI); and
- If conducted by a **health IT *developer***, exchange, or network, developer, exchange, or network ***knows, or should know***, that practice ***likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI***; or
- If conducted by a **health care provider**, provider ***knows*** that such practice is ***unreasonable*** and ***likely to interfere*** with, prevent, or materially discourage access, exchange, or use of electronic health information.

Information Blocking: Penalties and Enforcement

- Health Care Providers: Enforcement by CMS and the HHS OIG based on CMS incentive program attestations—*Penalties for false attestations*
- Health IT Developers, HIEs, HINs: Enforcement by ONC and/or HHS OIG—*Penalties for false attestations (certified developers) and up to $1 million civil monetary penalties (CMPs) per violation (developers, HIEs, HINs)*

In general enforcement per ONC Final Rule 6 months after Final Rule (CMPs – also after OIG proposed and final rule)

ONC Interoperability Final Rule: Information Blocking and Certification



RIN 0955-AA01 Page **1** of **1244**

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: Final rule.

SUMMARY: This final rule implements 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 will advance interoperability and support the access, exchange, and use of electronic health information. The rule also finalizes certain modifications to 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:

Effective Date: This final rule is effective on [insert 60 days after the date of publication in the **Federal Register**].

NOTICE

This HHS-approved document has been submitted to the Office of the Federal Register (OFR) for publication and has not yet been placed on public display or published in the Federal Register. The document may vary slightly from the published document if minor editorial changes have been made during the OFR review process and in the total number of pages due to the removal of this notice. The document published in the Federal Register is the official HHS-approved document.

Final Rule—and not Interim Final Rule with Comments or Supplemental Notice of Proposed Rulemaking, as some requested:

It has been three years since the Cures Act was enacted and information blocking remains a serious concern. This final rule includes provisions that will address information blocking and cannot be further delayed.

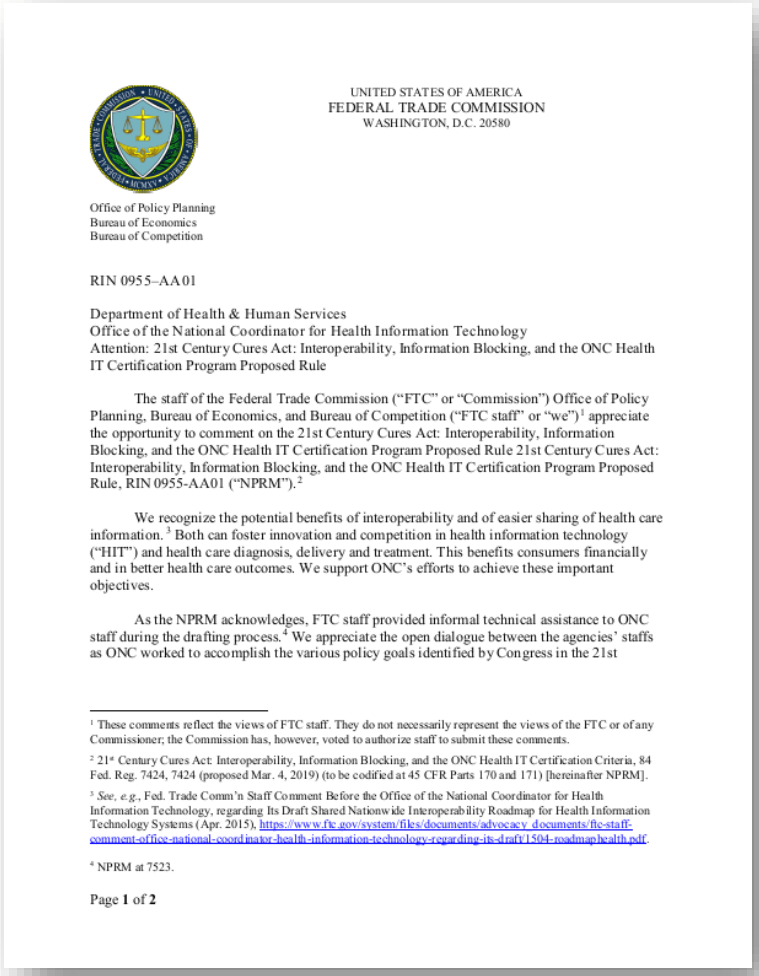
We have taken multiple actions to address some expressed concerns regarding the timing of the Conditions and Maintenance of Certification requirements as well as the comprehensiveness of the information blocking proposals.

We continue to receive complaints and reports alleging information blocking from a wide range of stakeholders.

ONC NPRM Public Comment Themes and Responses

- ✓ Significant burdens on actors
- ❖ Revise NPRM and submit for second set of comments
- ✓ Delay Effective Date to enable changes
- ✓ Clarify enforcement
- ✓ Exceptions: Categories right but some see loopholes, others as too restrictive
- ❖ Blocking defined too broadly
- ✓ HIE/HIN definitions confusing
- ✓ Narrow EHI definition; use ePHI
- ✓ Pricing/contracting too restrictive, excessive documentation, could distort markets
  - ✓ Final Rule relaxes, including in new Content & Manner Exception

FTC Comments on Proposed Rule Addressed



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Policy Planning
Bureau of Economics
Bureau of Competition

RIN 0955–AA01

Department of Health & 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

The staff of the Federal Trade Commission ("FTC" or "Commission") Office of Policy Planning, Bureau of Economics, and Bureau of Competition ("FTC staff" or "we")[1] appreciate the opportunity to comment on the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule, RIN 0955-AA01 ("NPRM").[2]

We recognize the potential benefits of interoperability and of easier sharing of health care information.[3] Both can foster innovation and competition in health information technology ("HIT") and health care diagnosis, delivery and treatment. This benefits consumers financially and in better health care outcomes. We support ONC's efforts to achieve these important objectives.

As the NPRM acknowledges, FTC staff provided informal technical assistance to ONC staff during the drafting process.[4] We appreciate the open dialogue between the agencies' staffs as ONC worked to accomplish the various policy goals identified by Congress in the 21st

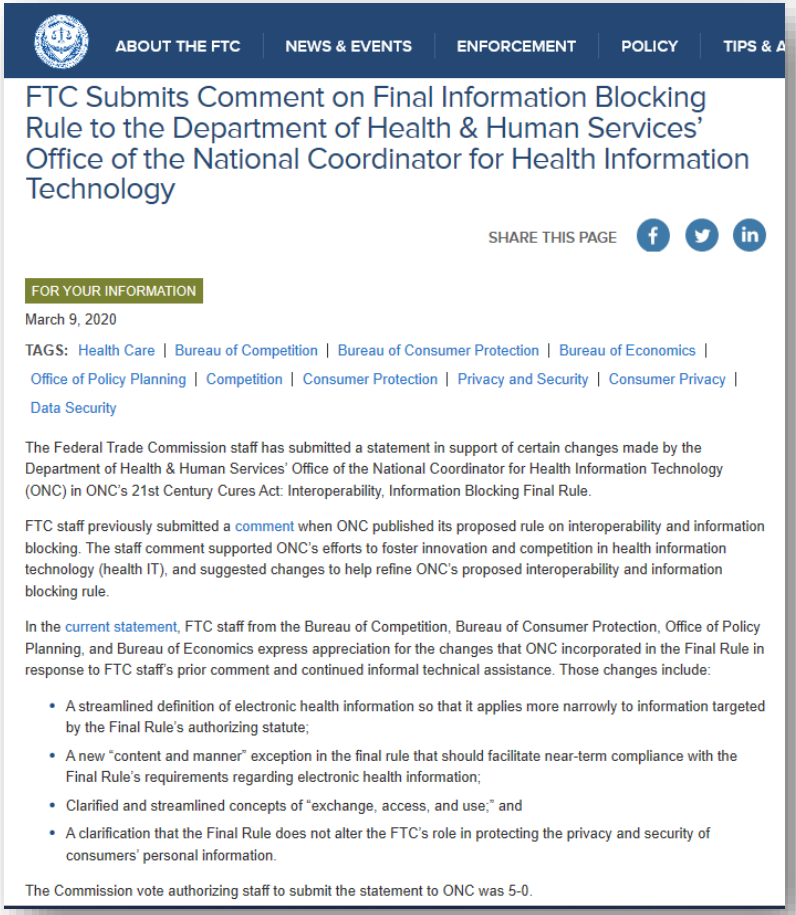
[1] These comments reflect the views of FTC staff. They do not necessarily represent the views of the FTC or of any Commissioner; the Commission has, however, voted to authorize staff to submit these comments.

[2] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Criteria, 84 Fed. Reg. 7424, 7424 (proposed Mar. 4, 2019) (to be codified at 45 CFR Parts 170 and 171) [hereinafter NPRM].

[3] *See, e.g.*, Fed. Trade Comm'n Staff Comment Before the Office of the National Coordinator for Health Information Technology, regarding Its Draft Shared Nationwide Interoperability Roadmap for Health Information Technology Systems (Apr. 2015), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-office-national-coordinator-health-information-technology-regarding-its-draft/1504-roadmaphealth.pdf.

[4] NPRM at 7523.

Page 1 of 2



ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & A

FTC Submits Comment on Final Information Blocking Rule to the Department of Health & Human Services' Office of the National Coordinator for Health Information Technology

SHARE THIS PAGE

FOR YOUR INFORMATION

March 9, 2020

TAGS: Health Care | Bureau of Competition | Bureau of Consumer Protection | Bureau of Economics | Office of Policy Planning | Competition | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

The Federal Trade Commission staff has submitted a statement in support of certain changes made by the Department of Health & Human Services' Office of the National Coordinator for Health Information Technology (ONC) in ONC's 21st Century Cures Act: Interoperability, Information Blocking Final Rule.

FTC staff previously submitted a comment when ONC published its proposed rule on interoperability and information blocking. The staff comment supported ONC's efforts to foster innovation and competition in health information technology (health IT), and suggested changes to help refine ONC's proposed interoperability and information blocking rule.

In the current statement, FTC staff from the Bureau of Competition, Bureau of Consumer Protection, Office of Policy Planning, and Bureau of Economics express appreciation for the changes that ONC incorporated in the Final Rule in response to FTC staff's prior comment and continued informal technical assistance. Those changes include:

- A streamlined definition of electronic health information so that it applies more narrowly to information targeted by the Final Rule's authorizing statute;
- A new "content and manner" exception in the final rule that should facilitate near-term compliance with the Final Rule's requirements regarding electronic health information;
- Clarified and streamlined concepts of "exchange, access, and use;" and
- A clarification that the Final Rule does not alter the FTC's role in protecting the privacy and security of consumers' personal information.

The Commission vote authorizing staff to submit the statement to ONC was 5-0.

Major Changes from Proposed Rule and Other Highlights: Information Blocking—Key Building Blocks

- **Timing and Enforcement**
  - Compliance date for information blocking six months after *Federal Register* publication
  - Delayed pending new compliance date and OIG CMP notice and comment (NPRM at OMB 1/23/2020)
- **HIE/HIN**
  - Combined and narrowed (but still broad applicability and ambiguity)
- **EHI (For Information Blocking and Otherwise)**
  - *Data elements* in USCDI for 24 months after publication
  - Then narrowed from Proposed Rule to ePHI in Designated Record Set
- **USCDI**
  - Data elements for information blocking six months after rule publication
  - Must implement in *certified HIT* within 24 months of publication
  - A few revisions from proposal but ONC did not accept most calls to expand v1
  - Among other sources, will look to HL7 FHIR "Patient Compartment" for possible expansion
- **Access, Exchange or Use; Interoperability Element**
  - Simplified and clarified
- **Certification**
  - Maintained use of *2015 edition*, with limited modifications
    - Eliminated several criteria, mostly as proposed
    - Revised referenced standards
    - Revised API criteria
  - Information blocking timing and other Conditions of Certification 6 months after rule publication

Major Changes from Proposed Rule and Other Highlights: Information Blocking—Exceptions

- Revised titles and content to simplify
- New Content and Manner Exception
  - Draws elements from proposed exceptions and relaxes fee and licensing exception impact
- Multiple other revisions but intent largely unchanged

ONC Final Rule: Key Dates

Actors Defined §171.102

Health Care Providers – *Finalized as Proposed*	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 – *Finalized with minor editorial revisions and one addition*	An individual or entity, other than a health care provider that self-develops health IT for its own use, that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj-11(c)(5) (ONC Health IT Certification Program). *Note: This explicit addition had been implied by other provisions of the proposed rule, which indicate that provider self-developers will be treated as providers for information blocking purposes.. ONC notes that self-developers will be subject to applicable certification provisions, including those related to information blocking.*

Actors Defined §171.102

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
Health Information Network or Health Information Exchange ***Revised in Final Rule and Combined***	*Health information network or health information exchange* means an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information: (1) Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and (2) That is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164. *ONC: "the narrower definition of HIN/HIE in this final rule should clearly exclude entities that might have been included under the proposed definitions, such as social networks, internet service providers, and technology that solely facilitates the exchange of information among patients and family members". Once an individual or entity is defined as an HIN or HIE, information subject to information blocking enforcement not limited to TPO.*

HIE and HIN

- ONC combined and narrowed two categories (e.g., removes "substantially influences")
- Focus on TPO only
- Maintained inclusion of "individual" as that term is in Cures
- Clarifies: must be exchange among more than two unaffiliated individuals or entities, *besides HIN/HIE*, that are enabled to exchange with each other
  - ONC states that revision ensures that definition does not unintentionally cover "essentially bilateral exchanges" in which intermediary "simply" performing a service on behalf of one entity in providing EHI to one or more entities and no "actual exchange" taking place among all entities (e.g., acting as intermediary between two entities where first sends non-standardized data to be converted by intermediary into standardized data for receiving entity)
- ONC retains, as proposed, as functional definition without specific exclusions
  - ONC notes that narrower definition of HIN/HIE should "clearly exclude entities that might have been included under proposed definitions (e.g., social networks, ISPs, and technology that solely facilitates exchange of information among patients and family members

Electronic Health Information Defined §171.102

- Electronic protected health information (defined in HIPAA) to the extent that it would be included in a designated record set ~~, 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~~
- As proposed, does not include de-identified health information
- Proposed Rule had an RFI on including price information within EHI with regard to information blocking; Final Rule says may or may not include price information, issue is whether it is PHI in a DRS

Electronic Health Information Defined §171.102

- Electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI shall not include:

  (1) Psychotherapy notes as defined in 45 CFR 164.501; or

  (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

  Note: Given narrower definition of EHI, term "observational health information" not used in the Final Rule. EHI limited to USCDI v1 for first 24 months via other Information Blocking and certification provisions

United States Core Data for Interoperability

FEBRUARY 2020 • VERSION 1

Table 1:
Data Class and Data Element Changed from NPRM
Data class is cell header. Data elements are bulleted.

Changed Data Elements NPRM to USCDI v1	
Proposed USCDI	**Final Cures Rule (USCDI v1)**
Patient Demographics • Address	**Patient Demographics** • Current Address • Previous Address • Phone Number • Phone Number Type • Email Address
Provenance • Author • Author Organization • Author Time Stamp	**Provenance** • Author Organization • Author Time Stamp
Substance Reactions* (including Medication Allergies) • Substance* • Reaction*	**Allergies and Intolerances** • Substance (Medication) • Substance (Drug Class) • Reaction

USCDI v1 Summary of Data Classes and Data Elements

Allergies and Intolerances
- Substance (Medication)
- Substance (Drug Class)
- Reaction

Assessment and Plan of Treatment
- Assessment and Plan of Treatment

Care Team Members
- Care Team Members

Clinical Notes
- Consultation Note
- Discharge Summary Note
- History & Physical
- Imaging Narrative
- Laboratory Report Narrative
- Pathology Report Narrative
- Procedure Note
- Progress Note

Goals
- Patient Goals

Health Concerns
- Health Concerns

Immunizations
- Immunizations

Laboratory
- Tests
- Values/Results

Medications
- Medications

Patient Demographics
- First Name
- Last Name
- Previous Name
- Middle Name (incl Middle Initial)
- Suffix
- Birth Sex
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Current Address
- Previous Address
- Phone Number
- Phone Number Type
- Email Address

Problems
- Problems

Procedures
- Procedures

Provenance
- Author Time Stamp
- Author Organization

Smoking Status
- Smoking Status

Unique Device Identifier(s) for a Patient's Implantable Device(s)
- Unique Device Identifier(s) for a Patient's Implantable Device(s)

Vital Signs
- Diastolic Blood Pressure
- Systolic Blood Pressure
- Body Height
- Body Weight
- Heart Rate
- Respiratory Rate
- Body Temperature
- Pulse Oximetry
- Inhaled Oxygen Concentration
- BMI Percentile (2 - 20 Years)
- Weight-for-length Percentile (Birth - 36 Months)
- Head Occipital-frontal Circumference Percentile (Birth - 36 Months)

Information Blocking: Key Definitions §171.102: Simplified

- *Access:* the ability or means necessary to make EHI available for exchange or 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~~ *[Note: transmission need not be one-way]*
- *Use:* the ability ~~of health IT or a user of health IT to access relevant~~ for electronic health information, once accessed or exchanged, to be understood and acted upon ~~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~~ *[Note: the general scope and meaning of the definition (e.g., write) is the same as proposed and use, like transmission, can be bi-directional]*

Interoperability Element §171.102: Simplified

- *Interoperability element* means hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that:

  (1) May be *necessary* to access, exchange, or use electronic health information; and

  (2) Is *controlled by the actor*, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of electronic health information.

Note: The first part of the definition draws on PHSA definition of health IT

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

Information Blocking Practices

- § 171.102: “an act or omission by an actor”
- Must be *likely to interfere with, prevent, or materially discourage* the access, exchange, or use of EHI
- ONC did not revise Proposed Rule examples but added *additional examples*
- ONC finalized purposes for access, exchange, or use for which interference will *almost always implicate* information blocking
- Focus on actors with *control* over interoperability elements

Business Associate Agreements: Final Rule Discussion

- "We designed the final rule to operate in a manner consistent with the framework of the HIPAA Privacy Rule and other laws providing privacy rights for patients. Foremost, we do not require the disclosure of EHI in any way that would not already be permitted under the HIPAA Privacy Rule (or other federal or state law). However, if an actor is *permitted* to provide access, exchange, or use of EHI under the HIPAA Privacy Rule (or any other law), then the information blocking provision would require that the actor provide that access, exchange, or use of EHI so long as the actor is not prohibited by law from doing so (assuming that no exception is available to the actor)."
- While the information blocking provision does not require actors to violate a BAA, a BAA or its associated service level agreements must not be used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule.
  - For example, a BAA entered into by one or more actors that permits access, exchange, or use of EHI by certain health care providers for treatment should generally not prohibit or limit the access, exchange, or use of the EHI for treatment by other health care providers of a patient.

Business Associate Agreements: Final Rule Discussion

- Both the provider(s) who initiated the BAA and the BA who may be an actor under the information blocking provision (e.g., a health IT developer of certified health IT) would be subject to the information blocking provision in the instance described above.
  - To illustrate the potential culpability of a BA, a BA with significant market power may have contractually prohibited or made it difficult for its covered entity customers to exchange EHI, maintained by the BA, with health care providers that use an EHR system of one of the BA's competitors.
  - To determine whether there is information blocking, the actions and processes (e.g., negotiations) of the actors in reaching the BAA and associated service level agreements would need to be reviewed to determine whether there was any action taken by an actor that was likely to interfere with the access, exchange, or use of EHI, and whether the actor had the requisite intent.
  - If the BA has an agreement with the covered entity to provide EHI to a third party that requests it and the BA refuses to provide the access, exchange, or use of EHI to a requestor in response to the request received by the CE, the BA (who is also an actor under the information blocking provision) may have violated the information blocking provision unless an exception applied.

Additional Edited ONC Examples in Final Rule: Restrictions on Access, Exchange, or Use That Might Implicate Information Blocking

- An actor (e.g., a health care provider that is a covered entity under HIPAA) may want to engage an entity for services (e.g., use of a clinical decision support application ("CDS App Developer")) that require the CDS App Developer to enter into a BAA with the health care provider and, in order to gain access and use of the EHI held by another BA of the health care provider (e.g., EHR developer of certified health IT), the CDS App Developer is required by the EHR developer of certified health IT to enter into a contract to access its EHR technology.
- An entity may offer an application that facilitates patients' access to their EHI through an API maintained by an actor (e.g., EHR developer of certified health IT) that is a BA of a health care provider that is a covered entity under HIPAA.
- A health care provider may request EHI from an actor that is a BA of another health care provider under HIPAA, such as an EHR developer of certified health IT or HIN, that is contracted to make EHI available for treatment purposes.

ONC clarifies: "contracts and agreements can interfere with the access, exchange, and use of EHI through terms besides those that specify unreasonable fees and commercially unreasonable licensing terms".

Additional Edited ONC Examples in Final Rule: Limiting or Restricting the Interoperability of Health IT

- Publication of "FHIR service base URLs" (i.e., "FHIR endpoints")
  - A FHIR service base URL cannot be withheld by an actor as it (just like many other technical interfaces) is necessary to enable the access, exchange, and use of EHI.
  - In the case of patients seeking access to their EHI, the public availability of FHIR service base URLs is an absolute necessity and without which the access, exchange, and use of EHI would be prevented. Thus, any action by an actor to restrict the public availability of URLs in support of patient access would be more than just likely to interfere with the access, exchange, or use of EHI; it would prevent such access, exchange, and use. Accordingly, as noted in § 170.404(b)(2), a Certified API Developer must publish FHIR service base URLs for certified API technology that can be used by patients to access their electronic health information.
- Slowing or delaying access, exchange, or use of EHI could constitute an "interference" and implicate information blocking provision; for example, scoping and architecture questions could constitute interference and implicate information blocking if they are not necessary to enable access, exchange, or use of EHI and are being utilized as a delay tactic

Additional Edited ONC Examples in Final Rule: Limiting or Restricting the Interoperability of Health IT

- An actor's refusal to register a software application that enables a patient to access their EHI would effectively prevent its use given that registration is a technical prerequisite for software applications to be able to connect to certified API technology
  - Such refusals in the context of patient access unless otherwise addressed in this rule would be highly suspect and likely to implicate information blocking
- There is often specific information that may be necessary for certain actors, such as health care providers, to effectively access, exchange, and use EHI via their Certified EHR Technology and certified Health IT Modules. A health care provider's "direct address" is an example of this kind of information.
  - If this information were not made known to a health care provider upon request, were inaccessible or hidden in a way that a health care provider could not identify (or find out) their own direct address, or were refused to be provided to a health care provider by a health IT developer with certified health IT, we would consider all such actions to be information blocking because knowledge of a direct address is necessary to fully engage in the exchange of EHI.
- To the extent that a legal transfer of IP to an individual or entity that is not an actor is intended to facilitate circumvention of the information blocking provision, *transfer itself* by an actor could be considered interference with the access, exchange, or use of EHI

Additional Edited ONC Examples in Final Rule: Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-Enabled Care Delivery

- Vetting and "education" re: apps
  - *This final rule also supports and strongly encourages providing individuals with information that will assist them in making the best choice for themselves in selecting a third-party application.*
  - Practices that purport to educate patients about the privacy and security practices of applications and parties to whom a patient chooses to receive their EHI may be reviewed by OIG or ONC, as applicable, if there was a claim of information blocking. However, we believe it is unlikely these practices would interfere with the access, exchange, and use of EHI if they meet certain criteria.
    - Foremost, the information provided by actors must focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology.
    - Second, this information must be factually accurate, unbiased, objective, and not unfair or deceptive.
    - Finally, the information must be provided in a non-discriminatory manner. For example, all third-party apps must be treated the same way in terms of whether or not information is provided to individuals about the privacy and security practices employed. To be clear, an actor may not prevent an individual from deciding to provide its EHI to a technology developer or app despite any risks noted regarding the app itself or the third-party developer.
  - For example, actors may establish processes where they notify a patient, call to a patient's attention, or display in advance (as part of the app authorization process with certified API technology) whether the third-party developer of the app that the patient is about to authorize to receive their EHI has attested in the positive or negative whether the third party's privacy policy and practices (including security practices such as whether the app encrypts the EHI) meet certain "best practices" set by the market for privacy policies and practices.
  - ONC provides minimum app privacy notice criteria and examples

App Privacy Notices: Minimum Criteria

At a minimum, as it relates to the above, all third-party privacy policies and practices should adhere to the following:

1) *The privacy policy is made publicly accessible at all times, including updated versions;*
2) *The privacy policy is shared with all individuals that use the technology prior to the technology's receipt of EHI from an actor;*
3) *The privacy policy is written in plain language and in a manner calculated to inform the individual who uses the technology;*
4) *The privacy policy includes a statement of whether and how the individual's EHI may be accessed, exchanged, or used by any other person or other entity, including whether the individual's EHI may be sold at any time (including in the future); and*
5) *The privacy policy includes a requirement for express consent from the individual before the individual's EHI is accessed, exchanged, or used, including receiving the*
6) *individual's express consent before the individual's EHI is sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction).*

Exceptions

Revised/Final Policy Considerations for Exceptions

1. Exceptions are limited to certain activities important to the successful functioning of the U.S. health care system, including *promoting public confidence in health IT infrastructure* by *supporting the privacy and security* of EHI, and *protecting patient safety and promoting competition and innovation* in health IT and its use to provide health care services to consumers
2. Each is intended to address a *significant risk that regulated individuals and entities* (i.e., health care providers, health IT developers of certified health IT, health information networks, and health information exchanges) *will not engage in these reasonable and necessary activities because of potential uncertainty* regarding whether they would be considered information blocking
3. Each is *intended to be tailored*, through *appropriate conditions*, so that it is *limited to the reasonable and necessary activities* that it is designed to exempt

Information Blocking: Finalized Exceptions

- ONC revised the exceptions per comments, framed as questions, added an eighth exception, provides more guidance and examples in the Preamble, and divides exceptions into two categories:
  1. Not fulfilling requests to access, exchange, or use EHI
  2. Procedures for fulfilling requests to access, exchange, or use EHI
- Documentation requirements are in final exception conditions
- Final Rule creates a safe-harbor approach: *Failure to meet conditions of an exception does not mean a practice is information blocking, only that it would not have guaranteed protection from CMPs or disincentives, and would be evaluated on case-by-case basis (e.g., for level of impact, intent, knowledge)*

"Required by Law" as Exclusion from Information Blocking

- Proposed rule distinguished between "required by law" (excluded) and "pursuant to law" (not excluded, e.g., HIPAA Privacy)
- In Final Rule, responding to comments:
  - *References to federal and state law include statutes, regulations, court orders, and binding administrative decisions or settlements, such as (at the Federal level) those from the FTC or the Equal Employment Opportunity Commission (EEOC). We further note that "required by law" would include tribal laws, as applicable.*
- Further addressed in Privacy Exception

Exceptions: Not Fulfilling Requests to Access, Exchange, or Use EHI

Preventing Harm Exception

- *Final Rule revises and aligns with HIPAA Privacy Rule harm standards (§ 164.524(a)(3))*
- 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
  - Note: focus on physical harm retained for *some* types of harm consistent with cross-walked HIPAA harm provision
- Practice must be no broader than necessary to substantially reduce the risk of harm practice is implemented to reduce
- Practice must implement an *organizational policy* that meets certain requirements *or* based on *individualized assessment of risk in each case*
  - Likely challenges to policies to delay release of test results to patients

§ 171.201 Preventing Harm Exception — When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking?

An actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm will not be considered information blocking when the practice meets the conditions in paragraphs (a) and (b) of this section, satisfies at least one condition (subparagraph) from each of paragraphs (c), (d) and (f) of this section, and also meets the condition in paragraph (e) of this section when applicable.

(a) *Reasonable belief.* The actor engaging in the practice must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information affected by the practice. For purposes of this section, "patient" means a natural person who is the subject of the electronic health information affected by the practice.

(b) *Practice breadth.* The practice must be no broader than necessary to substantially reduce the risk of harm that the practice is implemented to reduce.

(c) *Type of risk.* The risk of harm must:

(1) Be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination; *or*

(2) Arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

(d) *Type of harm.* The type of harm must be one that could serve as grounds for a covered entity (as defined in § 160.103 of this title) to deny access (as the term "access" is used in part 164 of this title) to an individual's protected health information under:

(1) Section 164.524(a)(3)(iii) of this title where the practice is likely to, or in fact does, interfere with access, exchange, or use (as these terms are defined in § 171.102) of the patient's EHI by their legal representative (including but not limited to personal representatives recognized pursuant to 45 CFR 164.502) and the practice is implemented pursuant to an individualized determination of risk of harm consistent with (c)(1) of this section;

(2) Section 164.524(a)(3)(ii) of this title where the practice is likely to, or in fact does, interfere with the patient's or their legal representative's access to, use or exchange (as these terms are defined in § 171.102) of information that references another natural person and the practice is implemented pursuant to an individualized determination of risk of harm consistent with paragraph (c)(1) of this section;

(3) Section 164.524(a)(3)(i) of this title where the practice is likely to, or in fact does, interfere with the patient's access, exchange, or use (as these terms are defined in § 171.102) of their own EHI, regardless of whether the risk of harm that the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (c)(2) of this section; or

Privacy Exception

- 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. Preconditions prescribed by ~~privacy~~ laws not satisfied;
  2. Health IT developer of certified health IT not covered by HIPAA [i.e., developer not a BA for a patient facing product or service] but that implement documented and transparent privacy policies;
  3. Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1) and (2) [unreviewable grounds for denying patient right of access]; or
  4. Respecting an individual's request not to share information.
- 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*
- ONC emphasizes that information blocking provision may require that actors provide access, exchange, or use of EHI in situations where the HIPAA Rules would not require access of similar information; the HIPAA Privacy Rule *permits*, but does not *require*, covered entities to disclose ePHI in most circumstances
- Some Documentation requirements aligned with OIG safe harbor and HIPAA Privacy Rule documentation requirements (sub-exception 1) and examples of EHR-based documentation provided

§ 171.202 Privacy Exception — When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy not be considered information blocking?

(b) *Sub-Exception – Precondition not satisfied.* To qualify for the exception on the basis that state or federal law requires one or more preconditions for providing access, exchange, or use of electronic health information have not been satisfied, the following requirements must be met—

(1) The actor's practice is tailored to the applicable precondition not satisfied, is implemented in a consistent and non-discriminatory manner, and either:

(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 to determine when the precondition would be satisfied and, as applicable, the steps that the actor will take to satisfy the precondition; and

(C) Are implemented by the actor, including by providing training on the policies and procedures; or

(ii) Are 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.

(2) If the precondition relies on the provision of a consent or authorization from an individual and the actor has received a version of such a consent or authorization that does not satisfy all elements of the precondition required under applicable law, the actor must:

(i) Use reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all required elements of the precondition or provide other reasonable assistance to the individual to satisfy all required elements of the precondition; and

(ii) Not improperly encourage or induce the individual to withhold the consent or authorization.

(3) For purposes of determining whether the actor's privacy policies and procedures and actions satisfy the requirements of subsections (b)(1)(i) and (b)(2) above when the actor's operations are subject to multiple laws which have inconsistent preconditions, they shall be deemed to satisfy the requirements of the subsections if the actor has adopted uniform privacy policies and procedures to address the more restrictive preconditions.

Security Exception

- An actor may implement measures to promote the security of EHI—Practice must be:
  - Directly related to safeguarding confidentiality, integrity, and availability of EHI
  - Tailored to specific security risks
  - Implemented in a consistent and non-discriminatory manner
  - implementing an organizational security policy that meets certain requirements or based on individualized determination regarding risk and response in each case
- ONC takes a *fact-based approach* to allow each actor to implement policies, procedures, and technologies appropriate for its size, structure, risks to individuals' EHI
- The intent is to prohibit practices that "purport to promote the security of EHI but that are unreasonably broad and onerous on those seeking access to EHI, not applied consistently across or within an organization, or otherwise may unreasonably interfere with access, exchange, or use of EHI"
- Would apply to security practices exceeding minimum HIPAA Security Rule conditions

Infeasibility Exception

- 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.)~~
- Conditions:
  1. Actor cannot fulfill the request for access, exchange, or use of EHI due to events beyond the actor's control, namely a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority;
  2. Actor cannot unambiguously segment the requested EHI from other EHI; or
  3. Infeasible under the circumstances as demonstrated by contemporaneous documentation consistent and non-discriminatory consideration of several revised factors *including new Content and Manner Exception (which includes some aspects of proposal like "reasonable alternative")* and whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of EHI to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship.
- Actor must ~~*timely*~~ *respond* to infeasible requests within ten business days of receipt of request
- Two factors that may not be considered in the determination: (1) whether the manner requested would have facilitated competition with the actor; and (2) whether the manner requested prevented the actor from charging a fee or resulted in a reduced fee.

Health IT Performance Exception

- 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
  - ONC notes that a period of health IT unavailability or performance degradation could be outside the parameters of SLAs without being "longer than necessary" in the totality of applicable circumstances and, therefore, without necessarily constituting information blocking as defined in § 171.103 [Unclear if exception still applies or this becomes a case-by-case issue]
- An actor must ensure that the health IT is unavailable for no longer than necessary to achieve the maintenance or improvements
- An actor may take action against a third-party application (including but not limited to patient-facing apps) that is negatively impacting the health IT's performance, provided that the practice is—(1) For a period of time no longer than necessary to resolve any negative impacts; (2) Implemented in a consistent and non-discriminatory manner; and (3) Consistent with existing SLAs, where applicable.
- Harm, Security, or Infeasibility (e.g., disaster)-related practices addressed by those respective exceptions

Exceptions: Procedures for Fulfilling Requests to Access, Exchange, or Use EHI

Content and Manner Exception (New)

- New exception, addressing some elements of proposed Feasibility Exception, with two alternative ("or") conditions
- *Content condition* –An actor must respond to request to access, exchange, or use electronic health information with
  - EHI in *USCDI data elements for* up to 24 months after Final Rule publication; and
  - On and after 24 months after publication date, a*ll EHI* as (re)defined in § 171.102
- *Manner condition*
  - *Manner requested*. (i) Actor must fulfill request per Content Condition in any manner requested, unless technically unable or *cannot reach terms with requestor* If actor fulfills such a request described in any manner requested:
    - **Any fees charged in fulfilling the response *need not* satisfy Fee Exception (i.e., could be "market rate); and**
    - **Any license of interoperability elements granted in fulfilling the request *need not* satisfy Licensing Exception**

Content and Manner Exception (New)

- *Alternative manner*. If actor does not fulfill request in any manner requested because technically unable or cannot reach terms with requestor (intended as a high bar), actor must fulfill request in an alternative manner, as follows:
  - Without unnecessary delay in following order of priority, starting with (A) and only proceeding to next consecutive paragraph if technically unable to fulfill request in manner identified in a paragraph.
    A. Using technology certified to standard(s) adopted in Part 170 (ONC certification) specified by requestor.
    B. Using content and transport standards specified by requestor and published by the Federal Government or an ANSI accredited SDO
    C. Using mutually agreeable alternative machine-readable format, including means to interpret EHI
  - Any fees charged by actor in fulfilling request must satisfy the Fee Exception
  - Any license of interoperability elements granted by the actor in fulfilling request must satisfy Licensing Exception
- If still unable to fulfill request, use Infeasibility Exception

Fees ~~Costs~~ Exception

- In setting fees for providing access, exchange, or use of EHI, an actor may charge fees, including a "reasonable profit margin," if they are:
  - charged on basis of *objective and verifiable criteria uniformly applied* to all ~~substantially similar~~ or similarly situated persons and requests;
  - *related to the costs* of providing access, exchange, or use; and
  - *reasonably allocated among all similarly situated ~~customers~~ persons or entities that* use the product/service [intended to allow approaches like sliding fee scales per comments]
  - based on costs not otherwise recovered for same instance of service to a provider and third party
  - not based in any part on whether requestor is a *competitor*, potential competitor, or will be using EHI to facilitate competition with the actor; and
  - not based on *sales, profit, revenue*, or other value requestor derives or may derive, ~~including secondary use of such information,~~ [intent remains] *that exceed the actor's reasonable costs*
  - not based on *costs that led to creation of IP, if the actor charged a royalty for that IP* per § 171.303 and royalty included development costs for IP creation
  - costs actor incurred due to the health IT being *designed or implemented in non-standard way,* unless requestor agreed to fees associated with non-standard approach
  - certain costs associated with *intangible assets* other than actual development or acquisition costs
  - *opportunity costs* unrelated to access, exchange, or use of EHI; or
  - based on *anti-competitive or other impermissible criteria*
- Costs excluded from exception: *some* data export, electronic access by individual to EHI, fees prohibited by 45 CFR 164.524(c)(4)) [HIPAA Privacy Rule]
- Health IT developers subject to Conditions of Certification on fees must comply with all requirements of such conditions for all practices and at all relevant times
- *Note: new Manner and Content Exception materially relaxes fee regulation*

Licensing Exception

- 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)*~~ *per conditions (uses concepts of reasonable and necessary in specific ways but not RAND model)*
  - *Negotiating a license* conditions: timeliness begin license negotiations with requestor within 10 business days from receipt of request and negotiate (in good faith) license within 30 business days from receipt
  - *Licensing* conditions: includes scope of rights; reasonable, non-discriminatory royalty and terms (including an actor may not charge a royalty for IP if the actor recovered any development costs pursuant to the Fee Exception that led to the creation of the IP); prohibited collateral terms; permitted NDA terms
  - *Additional conditions* relating to provision of interoperability elements to prohibit various forms of impeding licensee's efforts to use licensed elements
- ONC emphasizes in Final Rule that actor would *not need to license all of their IP* or license interoperability elements per this exception to a firm that requested a license solely for that firm's use in developing its own technologies and not to meet *current* needs for exchange, access or use of *EHI* to which it had a *"claim"* for *specific patients or individual access*
- ONC expects actors to take *immediate steps to come into compliance* with the information blocking provision by amending their contracts or agreements to eliminate or void any clauses that contravene the information blocking provision
- See Proposed Rule for *practices* that could implicate information blocking
- *Note: new Manner and Content Exception materially relaxes fee regulation*

Additional Issues

Requests for Information

- Additional Exceptions
  - ONC had asked whether it should propose, in future rulemaking, a narrow additional information blocking exception for practices needed to comply with TEFCA Common Agreement requirements
    - ONC did not add a new exception related to TEFCA participation in the Final Rule but noted that it received 40 comments on this RFI and may use this feedback in future rulemaking
  - ONC sought comment on potential new exceptions for future rules
    - In Final Rule, ONC addresses multiple comments for new exceptions and states finalized exceptions could address identified issues
- Disincentives for Health Care Providers
  - ONC asked 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
  - It received many comments for and against such incentives and their structure and extent—these have been shared with HHS agencies for consideration in future rulemaking

Complaint Process and Enforcement

- Cures directs ONC to implement a standard process to submit blocking claims
  - ONC has developed a dedicated complaint process based on experience with the process at https://www.healthit.gov/healthit-feedback and comments
  - ONC will implement ***and evolve*** this complaint process
- ONC's enforcement will focus on certification compliance with a *corrective action plan* approach and it has sole authority (relative to ONC-ACBs) Conditions/ Maintenance of Certification (including information blocking) via "direct review"
- HHS OIG has independent authority to investigate information blocking and false attestations by developers and other actors
- OIG can receive and review public complaints and will provide training to allow investigators to identify blocking allegations as part of fraud and abuse investigations
- OIG will establish policies and procedures to review and triage complaints
- ONC has finalized proposed approach to allow it to coordinate review of a claim of information blocking with OIG or defer to OIG to lead a claim review; finalized approach will also allow ONC to rely on OIG findings for basis of direct review action

Complaint Process and Enforcement

- ONC and OIG are actively coordinating on establishing referral policies and procedures to ensure timely and appropriate flow of information re: information blocking complaints
- They coordinated timing of final rule effective date and start of enforcement, including for Conditions of Certification related to information blocking (6 months from publication)
- CMP enforcement will not begin until set by future OIG notice and comment rulemaking (Proposed Rule at OMB since 1/23/2020)
  - Actors are not subject to CMPs until OIG rule final
- At a minimum, enforcement would not begin sooner than the compliance date of the information blocking provision (6 months after publication) and will depend on when the CMP rules finalized
- **Conduct before that time not subject to information blocking CMPs**

Timing and Other Revisions

*During this combined period of 24 months, ONC strongly encourages actors to apply the exceptions to all EHI as if the scope were not limited to EHI identified by the **data elements [not standards]** represented in the USCDI.*

ONC expects actors to use this 18-month delay from the compliance date of the information blocking section of this final rule (45 CFR part 171) (in addition to the 6-month period from the publication date of this final rule to the information blocking compliance date) to practice applying the exceptions to real-life situations and to update their processes, technologies, and systems to adapt to the new information blocking requirements.

ONC Certification and Information Blocking

Maintenance of Certification: Information Blocking

- Per Cures, ONC finalizes Conditions and Maintenance of Certification for 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 satisfy information blocking exceptions.*

Conditions of Certification: Information Blocking §170.401 – Finalized as Proposed

- As a *Condition of Certification (CoC)* and to maintain such certification, a health IT developer must not take any action that constitutes information blocking as defined in Cures
  - In some cases, these go beyond API certification criteria, for example, after 24 months, information blocking focuses on revised EHI definition rather than USCDI and *use* includes *write* and extends beyond the proposed new API certification criteria
  - Fee and transparency requirements are part of API CoC
- Provision subject to finalized information blocking exceptions
- No Maintenance of Certification beyond ongoing compliance
- This provision and several other new Conditions and Maintenance of Certification implemented six months after Final Rule publication

Conditions of Certification: Information Blocking: Assurances– Finalized With Revisions

- *Condition of Certification*: A health IT developer must provide assurances to the Secretary (unless for Exceptions) 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.
  - 170.402(a)(1) [information blocking] has six-month delayed compliance date
- A health IT developer must ensure its certified health IT conforms to full scope of the applicable certification criteria
- Developers of certified health IT must provide assurances they have made certified capabilities available in ways that enable them to be implemented and used in production for intended purposes
- ONC: Information blocking policies do not require providers to implement Health IT Modules certified to API technical requirements but other programs, like CMS MIPS and PIP, may require use of this technology

API: Read and Write

Certification

- As was proposed, final certification criterion only requires mandatory support for "read" access, though ONC anticipates that a future version of this criterion that could include "write" requirements (for example, to aid decision support) once FHIR-based APIs are widely adopted.
- ONC encourages industry to advance "write" capabilities and standards

Information Blocking

- Proposed Rule stated: *". . . '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.*
- Final Rule eliminated specific reference to "write" in "use" definition, but states:
  - " 'acted upon' within the final definition encompasses the ability to read, write, modify, manipulate, or apply the information from the proposed definition."
  - " 'use' is bi-directional. . . Thus, an actor's practice could implicate the information blocking provision not only if the actor's practice interferes with the requestor's ability to read the EHI (one-way), but also if the actor's practice interferes with the requestor's ability to write the EHI (bi-directional) back to a health IT system."

ONC Rule: Summing Up

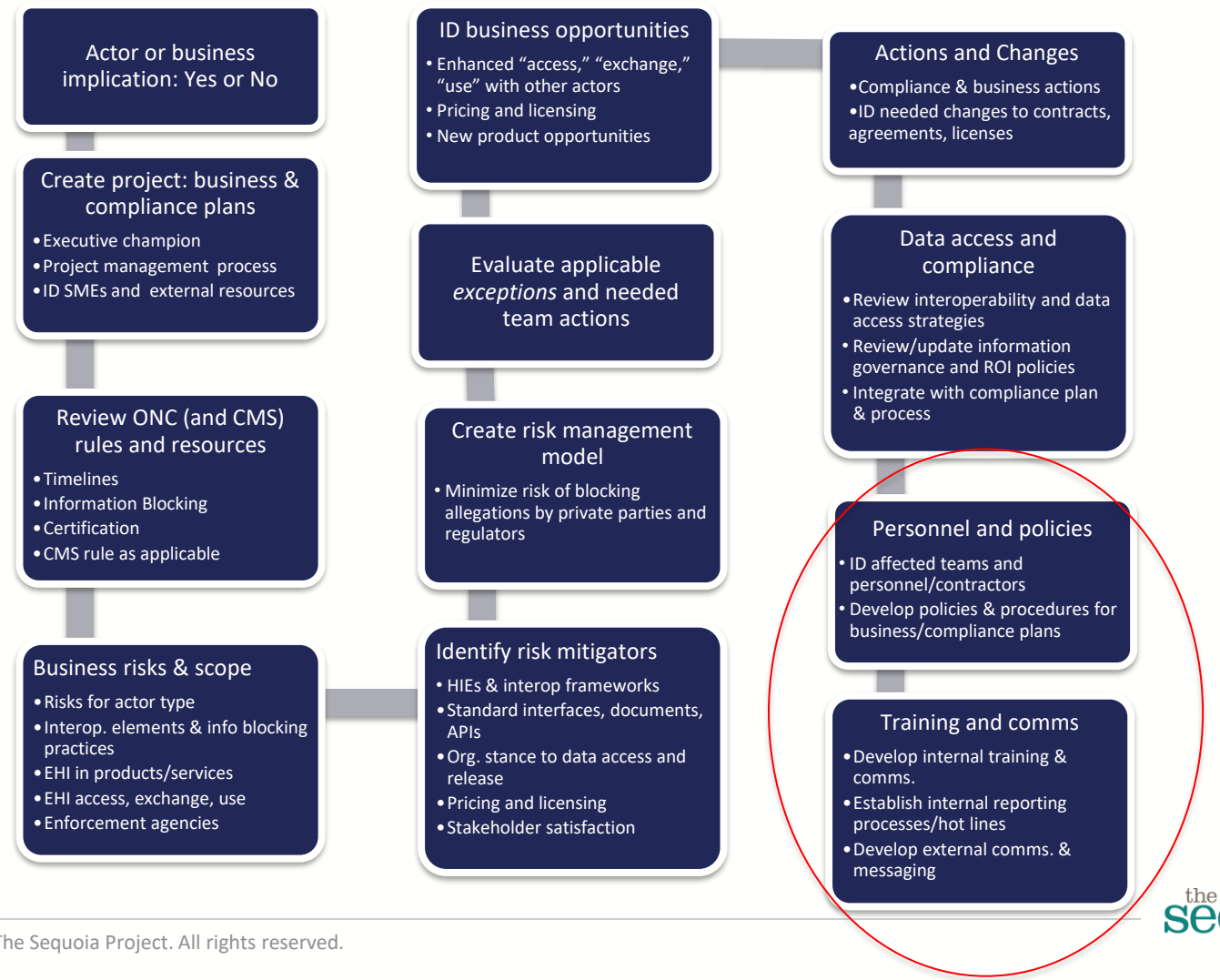
Information Blocking: Looking Ahead

- Final Rule retained key provisions but with material revisions, more flexibility and relaxed timing
- A few certification provisions effective 60 days after publication
- Information blocking compliance six months (or more) after publication, not sixty days
- Others: effective 24 months after Final Rule publication (e.g., USCDI v1, API technology criteria) or 36 months (i.e., EHI data export)

- ➢ Extended period of regulatory and compliance uncertainty
- ➢ Scarcity of qualified legal advice and lack of guidance and case law to support legal interpretations
- ➢ Community needs implementation guidance to meet legislative and regulatory intent and reduce compliance uncertainty and costs

Phase 3: Implementation Planning

Organization-Wide Information Blocking Plan: Overall Model



Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (1)

- ❑ Are you an "actor" and if so for which units of your organization?
  - ❑ If not, are you likely to have market or commercial implications from rule?
  - ❑ If "No" for either aspect of this question, STOP.
- ❑ If "Yes," create an organizational "information blocking" project or initiative
  - ❑ Business plans (e.g., product, engineering, marketing, commercial, legal, HR/training, communications, etc.)
  - ❑ Compliance plan (complement and integrate with business plans): primarily if "actor"
- ❑ Designate an overall senior executive project owner/champion
  - ❑ Designate business unit project owners as needed
- ❑ Establish a project management process (e.g., PMO)
  - ❑ Create projects as needed
- ❑ Identify/designate/train internal SMEs and project "champions" and influencers
  - ❑ Identify and mitigate staff misalignments between HIPAA focus on information protection and Cures focus on information sharing – may require cultural/professional reorientation
  - ❑ Create change management process for shift from HIPAA focus to HIPAA/Cures balance
- ❑ Identify external resources (legal, compliance, policy, training, etc.)
- ❑ Identify and engage with external industry resources (e.g., associations, interoperability initiatives, experts, colleagues, etc.)

Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (2)

- ❑ Review ONC proposed and rule
- ❑ Review ONC (and CMS) final rule, ONC website, industry resources
  - ❑ Compliance timelines
  - ❑ Information blocking provisions
  - ❑ As applicable, ONC certification provisions (developers and actors that expect to interact with ONC certified interoperability capabilities)
  - ❑ As applicable, CMS final rule (especially payors and health plans)
- ❑ Review OIG guidance and other material
- ❑ Review 2019 Stark/AKS proposed rules re: information blocking provisions
- ❑ Reconcile (sometimes conflicting) regulatory standards for data release: HIPAA (protect data) & Cures (share data/no information blocking)
  - Don't rely on providers' EHR/HIT vendors for this process – they cannot do it alone

Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (3)

- Identify business risks and scope:
  - Note: much of this risk assessment activity is standard practice or underway: fine tune after Final Rule
  - Risks specific to type of actor (e.g., developer, provider, HIE, HIN)
    - Developers have additional certification-related requirements/risks
    - Developers, HIEs, HINs have $1 M/violation maximum fines – need guidance on specifics, such as how "violation" defined
    - Providers: attest for QPP and subject to payment adjustments, OIG, Federal False Claims Act, etc.
  - Interoperability elements covered by organization
  - Applicable information blocking practices per:
    - Definition of information blocking
    - ONC-identified practices
    - ONC practice examples
  - EHI included in organization products or services
    - Implementation of standards for EHI (e.g., C-CDA, USCDI, HL7® FHIR®, etc.)
    - Non-standard EHI and how it can be made accessible
  - Potential external access, exchange, or use of EHI
    - Current and potential external EHI requesters
    - Consider academic (e.g., approved IRB) and private researcher requests and Business Associate requests
      - Note that IRB waiver access route is permitted but not required under HIPAA, patient authorization and/or HIPAA permitted purpose still required, and deidentified data (per HIPAA) is not EHI (and therefore not subject to information blocking prohibition)
  - Identify enforcement agencies: ONC, OIG, CMS, FTC, etc.
    - Review organization experience and relationships with agencies
  - Develop tailored scenarios for data access requests, apply regulation/guidance, seek guidance

Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (4)

- ❑ Identify risk mitigators, including:
  - ❑ Participation in HIEs and interoperability frameworks
  - ❑ Implementation of standard interfaces, document-types, APIs, messaging, etc.
  - ❑ Organizational stance toward data access and release of information
  - ❑ Pricing and licensing approaches
  - ❑ Stakeholder satisfaction with data sharing/access
    - ❑ Consider stakeholder surveys/outreach
- ❑ Develop a risk management model, such as is used for malpractice, to minimize the risk of allegations of information blocking by:
  - ❑ Private parties
  - ❑ Regulators

Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (5)

- ❑ Evaluate finalized applicable *exceptions* and needed actions by team: initial/ongoing
  - ❑ Preventing Harm: Legal, etc.
  - ❑ Privacy: Privacy officer, legal, etc.
  - ❑ Security: Security officer, legal, engineering, etc.
  - ❑ Infeasibility: Client services, product, engineering, etc.
    - ❑ Need process to identify and handle timely
  - ❑ Performance: CIO, engineering, legal, etc.
    - ❑ Need to review/revise SLAs
  - ❑ Content & Manner: Engineering, CFO, legal, licensing, pricing, product, marketing
  - ❑ Fees: CFO/accounting, pricing, marketing, legal, etc.
    - ❑ Evaluate costs and cost accounting and relationship to pricing
    - ❑ Specific CEHRT developer requirements re: APIs
    - ❑ Note: need more clarity/guidance on "reasonable" costs and fees
  - ❑ Licensing: legal, licensing, pricing, product, marketing
    - ❑ Identify licensed interoperability elements

Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (6)

- ❑ Identify business opportunities (even if not an "actor")
  - ❑ Enhanced "access," "exchange," "use" with other actors
    - ❑ e.g., access data from an EHR or HIE or to write to an EHR
  - ❑ Pricing and licensing opportunities
  - ❑ New product opportunities
  - ❑ Focus on identified consumer/patient needs

Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (7)

- ❑ Identify needed/desired compliance and business actions
  - ❑ Identify owners
  - ❑ Conduct and update gap analyses
- ❑ Identify needed changes to contracts, agreements, licenses
  - ❑ Develop process to revise: legal, commercial, client services
- ❑ Review interoperability and data access strategies, including use of:
  - ❑ Standards (HHS adopted, industry consensus, etc.)
  - ❑ APIs (FHIR and other)
  - ❑ Apps (developed by organization and those that connect with your HIT)
  - ❑ App stores, including licensing a pricing policies
  - ❑ Write access to your HIT by external apps/applications
- ❑ Review/update information governance and release of information policies
  - ❑ HIM and contractors

Organization-Wide Information Blocking Plan: Adapt to Actor-Type, Organizational Scale, and Organization (8)

- ❑ **Integrate with compliance plan and process**
- ❑ Identify affected teams and personnel, including contractors
  - ❑ Likely very wide across the organization
- ❑ Develop policies and procedures reflecting business and compliance plans
  - ❑ Including documentation of actions and events
- ❑ Develop internal training and communications process
  - ❑ Track and document training by relevant team members
- ❑ Establish internal reporting processes/hot lines
  - ❑ Concerns with information blocking risk
    - ❑ Internal
    - ❑ External (e.g., business partners, competitors, etc.)
  - ❑ Reporting mentions of "information blocking" in commercial or other external discussions
- ❑ Develop external communications and messaging strategy
  - ❑ General on organization approach to information blocking/interoperability
  - ❑ Focus on identified consumer/patient needs
  - ❑ Addressing public complaints

Additional Phase 3 Priorities and Next Steps

Additional Phase 3 Priorities: From January 2020 Call

- ❑ Review the ONC Final Rule
  - ❑ Provide implementation/compliance guidance and education
- ❑ Seek sub-regulatory guidance from HHS
  - ❑ OIG/ONC guidance/clarification re: information blocking status of data requests from researchers and industry, especially IRB waiver requests and data partnership requests/business associates
- ❑ Seek questions from the public, perhaps through a dedicated email box; aggregate/submit to HHS/OIG/ONC
- ❑ Address consumer/patient need for clarity re: information blocking
- ❑ Identify/develop priority scenarios; work with agencies on clarity
- ❑ Provide implementation guidance and resource materials

Closing Discussion and Next Steps

- Continue to Review Final Rule
  - Implementation, compliance, educational needs
- Communicate to ONC and OIG as needed in 2020
- Calls scheduled through May 2020

Interoperability Matters

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

Appendix 1:
Developing a Compliance Framework for the Information Blocking Rule

Information Blocking Compliance

- Actors will need to prepare for enforcement of the Information Blocking Rule by ONC and the OIG
- Assuring compliance with the Information Blocking Rule is a key part of this effort
- Compliance programs emerged in healthcare in the 1990s in response to federal government investigations
- Health care providers, payors, HINs and software developers approach compliance differently
- Compliance is often “siloed” in different parts of the organization.
  - Fraud and Abuse compliance is in one department, HIPAA compliance is in another department, technology compliance in yet another department
- Information Blocking cuts across different parts of the organization, which makes compliance a challenge

OIG Compliance Program Framework – Seven Elements

1. Written standards of conduct that affirm organization's commitment to achieving and maintaining compliance
2. Designation of a corporate compliance officer and other bodies that report directly to the CEO and governing body
3. Regular and effective education and training for staff
4. Implement a complaint process that protects anonymity of the person reporting, e.g. "hotline"
5. Effective response to complaints and discipline of those who break rules
6. Monitoring the compliance program for effectiveness
7. Investigate and remediate systemic problems

Information Blocking Compliance Framework

Element #1 - Written standards of conduct that affirm organization's commitment to achieving and maintaining compliance

COMMENTS

Confusion about what this means

Concerns about the burden on smaller organizations that may lack the resources to develop these materials

Information Blocking Compliance Framework

Element #2 - Designation of a corporate compliance officer and other bodies that report directly to the CEO and governing body

COMMENTS

Who is the “owner” of Information Blocking?

Do current compliance officers have the expertise?

Information Blocking Compliance Framework

Element #3 - Regular and effective education and training for staff

COMMENTS

- Actors will need time after publication of the Final Rule to ramp up their compliance efforts before enforcement actions begin
- Education must extend beyond the Actor's staff and include customers, partners, vendors and others

Information Blocking Compliance Framework

Element #4 - Implement a complaint process that protects anonymity of the person reporting, e.g. “hotline”

COMMENTS

No specific comments

Information Blocking Compliance Framework

Element #5 - Effective response to complaints (internal and external) and discipline of those who break rules

COMMENTS-

Will compliance with the Information Blocking Rule favor larger Actors and disadvantage smaller Actors?

Information Blocking Compliance Framework

Element #6 - Monitoring the compliance program for effectiveness

COMMENTS

No specific comments

Information Blocking Compliance Framework

Element #7 - Investigate and remediate systemic problems

COMMENTS

No specific comments

Issues for Continued Discussion

- Additional thoughts about how your organization plans to approach compliance with the information blocking rule
- Are there specific things about the information blocking rule that will make it more difficult to incorporate into your existing compliance programs?
- Other?

Appendix 2: Back-Up Material on ONC Final Rule

Practices

Practices: Selected, Edited ONC Examples

Restrictions on Access, Exchange, or Use

- Requiring consent to exchange EHI for treatment even though not required by law
- Developer refuses to share technical information needed to export data
- HIN restriction on end-user sharing EHI with non-HIN members
- Vendor only provides EHI in PDF on termination of customer agreement
- Developer of certified health IT refuses to license interoperability elements reasonably necessary for others to develop and deploy software that works with health IT

Practices: Selected, Edited ONC Examples
Limiting or Restricting the Interoperability of Health IT

- Actor deploys technological measures that restrict ability to reverse engineer to develop means for extracting and using EHI in the technology
- Hospital directs EHR developer to configure technology so users cannot easily send electronic referrals to unaffiliated providers, even when the user knows Direct address and/or identity of the unaffiliated provider
- Developer prevents (e.g., by exorbitant fees unrelated to costs or by technology) third-party CDS app from writing EHI to EHR as requested by provider
- Provider has capability to provide same-day access to EHI but takes several days to respond

Practices: Selected, Edited ONC Examples

Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-Enabled Care Delivery

- Developer of certified health IT requires third-party apps to be “vetted” for security but does not vet promptly
- Developer of certified health IT refuses to license interoperability elements that other applications require to access, exchange, and use EHI in the developer’s technology
- Provider engages integrator to develop interface engine but its license with EHR developer prohibits it from disclosing technical documentation integrator needs to perform the work [without broad non-compete]
- Health system insists local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and threatens to revoke admitting privileges for physicians that do not comply
- HIN charges additional fees, requires more stringent testing or certification requirements, or imposes additional terms for participants that are competitors, are potential competitors, or may use EHI obtained via the HIN in a way that facilitates competition with the HIN

Practices: Selected, Edited ONC Examples

Rent-Seeking and Other Opportunistic Pricing Practices

- Developer of certified health IT charges customers a fee exceeding their costs for interfaces, connections, data export, data conversion or migration, other interoperability services
- Developer of certified health IT charges more to export or use EHI in certain competitive situations or purposes
- Developer of certified health IT interposes itself between customer and third-party developer, insisting that developer pay licensing fee, royalty, or other payment [not related to costs] for permission to access EHR or documentation
- Analytics company provides services to customers of developer of certified health IT and developer insists on revenue sharing that exceeds its reasonable costs

ONC made no additions in Final Rule and points to Cost Exception for clarification

Practices: Selected, Edited ONC Examples

Non-Standard Implementation Practices

- Actor chooses not to adopt, or to materially deviate from, relevant standards, implementation specifications, and certification criteria adopted by the Secretary
- Even where no federally adopted or identified standard exists, if a particular implementation approach has been broadly adopted in a relevant industry segment, deviations from that approach would be suspect unless strictly necessary to achieve substantial efficiencies.
- Developer of certified health IT implements C-CDA for TOC summary receipt but only sends summaries in a proprietary or outmoded format
- Developer of certified health IT adheres to “required” portions of widely adopted standard but implements proprietary approaches for “optional” parts of the standard when other interoperable means are available

ONC made no additions in the Final Rule

Finalized Exceptions (Pages Not in Main Presentation)

Information Blocking: Exceptions

- Cures authorizes HHS Secretary to identify *reasonable and necessary* activities that are not information blocking
- *Practices* that are reasonable and necessary and not information blocking *if all applicable conditions* of exception satisfied *at all relevant times, for each practice* for which exception sought
- If actions of an *actor satisfy one or more exception*, *would not be treated as information blocking* nor subject to civil penalties/other disincentives—most apply to all actors, unless otherwise indicated
- Consistent ONC themes (e.g., pro-competitive, consistent, non-discriminatory, policies in place, documented compliance)
- The actor has burden of proving compliance if an investigation

§ 171.201 Preventing Harm Exception — When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking?

(4) Section 164.524(a)(3)(i) of this title where the practice is likely to, or in fact does, interfere with a legally permissible access, exchange, or use (as these terms are defined in § 171.102) of EHI not described in subparagraph (1), (2), or (3) of this paragraph, and regardless of whether the risk of harm the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (c)(2) of this section.

(e) *Patient right to request review of individualized determination of risk of harm.* Where the risk of harm is consistent with paragraph (c)(1) of this section, the actor must implement the practice in a manner consistent with any rights the individual patient whose EHI is affected may have under § 164.524(a)(4) of this title, or any federal, state, or tribal law, to have the determination reviewed and potentially reversed.

(f) *Practice implemented based on an organizational policy or a determination specific to the facts and circumstances.* The practice must be consistent with an organizational policy that meets subparagraph (1) of this paragraph or, in the absence of an organizational policy applicable to the practice or to its use in particular circumstances, the practice must be based on a determination that meets subparagraph (2) of this paragraph.

(1) An organizational policy must:

(i) Be in writing;

(ii) Be based on relevant clinical, technical, and other appropriate expertise;

(iii) Be implemented in a consistent and non-discriminatory manner; and

(iv) Conform each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use.

- (2) A determination must:
- (i) Be based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use; and
- (ii) Be based on expertise relevant to implementing the practice consistent with the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use in particular circumstances.

§ 171.202 Privacy Exception — When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy not be considered information blocking?

An actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy will not be considered information blocking when the practice meets all of the requirements of at least one of the sub-exceptions in paragraphs (b) through (e) of this section.

(a) *Definitions in this section*.

(1) The term *HIPAA Privacy Rule* as used in this section means 45 CFR Parts 160 and 164.

(2) The term *individual* as used in this section means one or more of the following—

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

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

(iii) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section in making decisions related to health care as a personal representative, in accordance with 45 CFR 164.502(g).

(iv) 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.

(v) 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.

§ 171.202 Privacy Exception — When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy not be considered information blocking?

(c) *Sub-exception – 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's organizational privacy policies must have been disclosed to the individuals and entities that use the actor's product or service before they agreed to use them, and must implement the practice according to a process described in the organizational privacy policies. The actor's organizational privacy policies must:

(1) Comply with state and federal laws, as applicable;

(2) Be tailored to the specific privacy risk or interest being addressed; and

(3) Be implemented in a consistent and non-discriminatory manner.

(d) *Sub-exception – Denial of an individual's request for their electronic health information consistent with 45 CFR 164.524(a)(1) and (2).* If an individual requests electronic health information under the right of access provision under 45 CFR 164.524(a)(1) from an actor that must comply with 45 CFR 164.524(a)(1), the actor's practice must be consistent with 45 CFR 164.524(a)(2).

§ 171.202 Privacy Exception — When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy not be considered information blocking?

(e) *Sub-exception – Respecting an individual's request not to share information*. Unless otherwise required by law, an actor may elect not to provide access, exchange, or use of an individual's electronic health information if the following requirements are met—

(1) The individual requests that the actor not provide such access, exchange, or use of electronic health information without any improper encouragement or inducement of the request by the actor;

(2) The actor documents the request within a reasonable time period;

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

(4) An actor may terminate an individual's request for a restriction to not provide such access, exchange, or use of the individual's electronic health information only if:

(i) The individual agrees to the termination in writing or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented by the actor; or

(iii) The actor informs the individual that it is terminating its agreement to not provide such access, exchange, or use of the individual's electronic health information except that such termination is:

(1) Not effective to the extent prohibited by applicable federal or state law; and

(2) Only applicable to electronic health information created or received after the actor has so informed the individual of the termination. [Note: Preamble links to needs for emergent needs for information sharing but the final language seems insufficient for that purpose]

§ 171.203 Security Exception — When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information not be considered information blocking?

An actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information will not be considered information blocking when the practice meets the conditions in paragraphs (a), (b), and (c) of this section, and in addition meets either the condition in paragraph (d) of this section or the condition in paragraph (e) of this section.

(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 be directly responsive 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 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.

§ 171.204 Infeasibility Exception — When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be considered information blocking?

An actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request will not be considered information blocking when the practice meets one of the conditions in paragraph (a) and meets the requirements in paragraph (b).

(a) *Conditions*. (1) *Uncontrollable events*. The actor cannot fulfill the request for access, exchange, or use of electronic health information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.

(2) *Segmentation*. The actor cannot fulfill the request for access, exchange, or use of electronic health information because the actor cannot unambiguously segment the requested electronic health information from electronic health information that:

(i) Cannot be made available due to an individual's preference or because the electronic health information cannot be made available by law; or

(ii) May be withheld in accordance with section 201 of this part.

§ 171.204 Infeasibility Exception — When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be considered information blocking?

(3) *Infeasible under the circumstances*. (i) The actor demonstrates, prior to responding to the request pursuant to paragraph (b) of this section, through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:

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

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

(C) The financial and technical resources available to the actor;

(D) Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(E) 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; and

(F) Why the actor was unable to provide access, exchange, or use of EHI consistent with the exception in § 171.301.

(ii) In determining whether the circumstances were infeasible under paragraph (3)(i) of this section, it shall not be considered whether the manner requested would have:

(A) Facilitated competition with the actor.

(B) Prevented the actor from charging a fee or resulted in a reduced fee.

(b) *Responding to requests*. If an actor does not fulfill a request for access, exchange, or use of electronic health information for any of the reasons provided in paragraph (a) of this section, the actor must, within ten business days of receipt of the request [was "timely], provide to the requestor in writing the reason(s) why the request is infeasible.

§ 171.205 Health IT Performance Exception — When will an actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information not be considered information blocking?

An actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information will not be considered information blocking when the practice meets a condition in paragraph (a), (b), (c), or (d) of this section, as applicable to the particular practice and the reason for its implementation.

(a) *Maintenance and improvements to health IT*. When an actor implements a practice that makes health IT under that actor's control temporarily unavailable, or temporarily degrades the performance of health IT, in order to perform maintenance or improvements to the health IT, the actor's practice must be —

(1) Implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;

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

(3) If the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN:

(i) *Planned*. Consistent with existing service level agreements between the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT; or

(ii) *Unplanned*. Consistent with existing service level agreements between the individual or entity; or 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) *Assured level of performance.* An actor may take action against a third-party application that is negatively impacting the health IT's performance, provided that the practice is—

(1) For a period of time no longer than necessary to resolve any negative impacts;

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

(3) Consistent with existing service level agreements, where applicable.

(c) *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.

(d) *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.

§ 171.301 Content and Manner Exception — When will an actor's practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information not be considered information blocking?

An actor's practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information will not be considered information blocking when the practice meets all of the following conditions.

(a) *Content condition – electronic health information.* An actor must respond to a request to access, exchange, or use electronic health information with—

(1) *USCDI.* For up to [Insert date 24 months after the publication date of the final rule], at a minimum, the electronic health information identified by the data elements represented in the USCDI standard adopted in § 170.213.

(2) *All electronic health information.* On and after [Insert date 24 months after the publication date of the final rule], electronic health information as defined in § 171.102.

(b) *Manner condition*. (1) *Manner requested*. (i) An actor must fulfill a request described in paragraph (a) of this section in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

(ii) If an actor fulfills a request described in paragraph (a) of this section in any manner requested:

(A) Any fees charged by the actor in relation to its fulfilling the response are not required to satisfy the exception in § 171.302; and

(B) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303.

(2) *Alternative manner*. If an actor does not fulfill a request described in paragraph (a) of this section in any manner requested because it is technically unable to fulfill the request or cannot

reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner, as follows:

(i) The actor must fulfill the request without unnecessary delay in the following order of priority, starting with paragraph (A) and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in a paragraph.

(A) Using technology certified to standard(s) adopted in part 170 that is specified by the requestor.

(B) Using content and transport standards specified by the requestor and published by:

(1) The Federal Government; or

(2) A standards developing organization accredited by the American National Standards Institute.

(C) Using an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor.

(ii) Any fees charged by the actor in relation to fulfillment of the request are required to satisfy the exception in § 171.302.

(iii) Any license of interoperability elements granted by the actor in relation to fulfillment of the request is required to satisfy the exception in § 171.303.

§ 171.302 Fees Exception — When will an actor's practice of charging fees for accessing, exchanging, or using electronic health information not be considered information blocking?

An actor's practice of charging fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using electronic health information will not be considered information blocking when the practice meets the conditions in paragraph (a), does not include any of the excluded fees in paragraph (b), and, as applicable, meets the condition in paragraph (c). The following definition applies to this section:

Electronic access means an internet-based method that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request.

(a) *Basis for fees condition.* (1) The fees an actor charges must be—

(i) Based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;

(ii) Reasonably related to the actor's costs of providing the type of access, exchange, or use of electronic health information to, or at the request of, the person or entity to whom the fee is charged;

(iii) Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported; and

(iv) Based on costs not otherwise recovered for the same instance of service to a provider and third party.

(2) The fees an actor charges must not be based on—

(i) 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;

(ii) Sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, or use of the electronic health information;

§ 171.302 Fees Exception — When will an actor's practice of charging fees for accessing, exchanging, or using electronic health information not be considered information blocking?

(iii) Costs the actor incurred due to the health IT being designed or implemented in a non-standard way, unless the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use the electronic health information;

(iv) Costs associated with intangible assets other than the actual development or acquisition costs of such assets;

(v) Opportunity costs unrelated to the access, exchange, or use of electronic health information; or

(vi) Any costs that led to the creation of intellectual property, if the actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.

(b) *Excluded fees condition.* This exception does not apply to—

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

(2) A fee based in any part on the electronic access of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual;

(3) 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; and

(4) A fee to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired.

(c) *Compliance with the Conditions of Certification condition.* 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), § 170.404, or both of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

§ 171.303 Licensing Exception — When will an actor's practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?

An actor's practice to license interoperability elements for electronic health information to be accessed, exchanged, or used will not be considered information blocking when the practice meets all of the following conditions.

(a) *Negotiating a license conditions.* Upon receiving a request to license an interoperability element for the access, exchange, or use of electronic health information, the actor must—

(1) Begin license negotiations with the requestor within 10 business days from receipt of the request; and

(2) Negotiate a license with the requestor, subject to the licensing conditions in paragraph (b) of this section, within 30 business days from receipt of the request.

(b) *Licensing conditions.* The license provided for the interoperability element(s) needed to access, exchange, or use electronic health information must meet the following conditions:

(1) *Scope of rights*. The license must provide all rights necessary to:

(i) Enable the access, exchange, or use of electronic health information; and

(ii) Achieve the intended access, exchange, or use of electronic health information via the interoperability element(s).

(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 (c)(3) of this section.

§ 171.303 Licensing Exception — When will an actor's practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?

(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 developing organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on terms consistent with those in this exception, the actor may charge a royalty that is consistent with such policies.

(iv) An actor may not charge a royalty for intellectual property if the actor recovered any development costs pursuant to § 171.302 that led to the creation of the intellectual property.

(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 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.

(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.

§ 171.303 Licensing Exception — When will an actor's practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?

(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 § 171.302.

(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 conditions 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.

Original Exceptions in Proposed Rule

~~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~~

~~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~~

~~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: 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: 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.~~

~~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: 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.~~ **[Removed in its entirety from the Final Rule]**

ONC Certification and Information Blocking (Additional Slides)

Conditions of Certification: Information Blocking Related– Finalized With Revisions

- 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 36 ~~24~~ months of final rule ~~effective~~ publication 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, 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

EHI Data Export and Information Blocking

- *. . . while that scope of EHI [as revised in Final Rule] may be comprehensive for that product [for which new EHI Export criterion applies], it may still not be all of the health information for which a health care provider is the steward and that meets the EHI definition within the health IT products deployed within their organization. . . . We note all of these distinctions to . . . dissuade readers from jumping to an improper conclusion that the EHI export criterion in the Certification Program is a substitute for or equivalent to the EHI definition for the purposes of information blocking. . . . Unless a health care provider (which is an "actor" regulated by the information blocking provision) only used a single health IT product to store EHI that was also certified to this certification criterion, the EHI definition will always be larger.*

- *In consideration of comments, the finalized "EHI export" criterion in § 170.315(b)(10) is not included in the 2015 Edition Base EHR definition, . . . We revised the policy in recognition of comments received, including comments regarding the structure and scope of the criterion as proposed and the development burden of the criterion. . . . including this certification criterion in the Conditions and Maintenance of Certification is the best place to include the requirement associated with the criterion. Thus, we have finalized the § 170.315(b)(10) certification criterion as a general certification requirement for the ONC Health IT Certification Program . . .*

Conditions of Certification: Application Programming Interfaces (APIs) §170.404

- Apply to actors per refined final definitions:
  - ~~*API Technology Suppliers*~~ Certified API Developer: health IT developer that creates certified API technology certified to any of certification criteria in § 170.315(g)(7) - (10)
  - *API* ~~*Data Provider*~~ Information Source*:* organization that deploys certified API technology created by a Certified API Developer
  - *API User*: API User means a person or entity that creates or uses software applications interacting with 'certified API technology' developed by a 'Certified API Developer' and deployed by an API Information Source directly (e.g., to develop third-party apps/services) or indirectly (e.g., user of third-party app/service)
- *Transparency*: Certified API Developers (Developers) must publish all API terms and conditions (including fees in detailed, plain language) and make business and technical documentation necessary to interact with their APIs freely and publicly accessible
  - Certified API Developer would be permitted to include consumer protections (e.g., how EHI will be used) in Ts and Cs documentation
- *Permitted fees*: ONC has finalized detailed conditions that govern fees that Developers could charge and to whom fees could be charged – detailed record keeping needed (ONC rejects negative comments)
  - Certified API Developers and API Users can collaborate and form relationships, so long as these relationships do not conflict with any provisions of Final Rule or other applicable federal and state laws and regulations
  - Sets boundaries for fees Certified API Developers are permitted to charge and to whom the fees can be charged, does not prohibit who may pay the permitted fee.
- *Pro-competitive*: ONC finalized that Developers must comply with requirements to promote an open and competitive marketplace

Application Programming Interfaces §170.404

Conditions of Certification

- Required by Cures
- 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 per applicable law
- Through APIs, developer must also provide access to all data elements (i.e., USCDI and associated specified FHIR resources) of a patient's EHR to the extent permissible under applicable privacy laws
- Note: EHI is broader than USCDI after 24 months
- Certified API Developer must publish Ts and Cs (including fees) and make business and technical documentation necessary to interact with their APIs in production freely and publicly accessible via a hyperlink
- All fees related to API technology, not otherwise permitted by this section, are prohibited from being imposed by a Certified API Developer (examples in Proposed Rule)
- Certified API Developers must grant API Information Sources (i.e., providers who purchase/license API technology) ~~sole authority and autonomy~~ independent ability to permit API Users to interact with API technology

Maintenance of Certification

- API Technology Suppliers must verify authenticity of application developers, within ~~five~~ ten business days of receipt of a request to register a developer's software with API technology
  - An API Information Source could show a warning to patients as part of the patient authorization for an application to receive their EHI from an API Information Source (could include a warning that an application attempting to access data on behalf of a patient is untrusted)
- A Certified API Developer must register and enable all applications for production use within ~~one five~~ business days of completing its verification of an applications developer's authenticity
- A Developer must support publication of "Service Base URLs" (i.e., FHIR® server endpoints) necessary to support patient access for all of its customers, regardless of those that are centrally managed by the Supplier or locally deployed by an API Information Source, and make such information publicly available at no charge

Application Programming Interfaces: Fees §170.404

(B) *API fees.* Any and all fees charged by a Certified API Developer for the use of its certified 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.

(3) *Fees conditions*. (i) *General conditions*. (A) All fees related to certified API technology not otherwise permitted by this section are prohibited from being imposed by a Certified API Developer. The permitted fees in paragraphs (a)(3)(ii) and (a)(3)(iv) of this section may include fees that result in a reasonable profit margin in accordance with § 171.302.

(B) For all permitted fees, a Certified API Developer must:

(*1*) Ensure that such fees are based on objective and verifiable criteria that are uniformly applied to all similarly situated API Information Sources and API Users;

(*2*) Ensure that such fees imposed on API Information Sources are reasonably related to the Certified API Developer's costs to supply certified API technology to, and if applicable, support certified API technology for, API Information Sources;

(*3*) Ensure that such fees to supply and, if applicable, support certified API technology are reasonably allocated among all similarly situated API Information Sources; and

(*4*) Ensure that such fees are not based on whether API Information Sources or API Users are competitors, potential competitors, or will be using the certified API technology in a way that facilitates competition with the Certified API Developer.

(C) A Certified API Developer is prohibited from charging fees for the following:

(*1*) Costs associated with intangible assets other than actual development or acquisition costs of such assets;

(*2*) Opportunity costs unrelated to the access, exchange, or use of electronic health information; and

(*3*) The permitted fees in this section cannot include any costs that led to the creation of intellectual property if the actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.

(D) *Record-keeping requirements*. A Certified API Developer must keep for inspection detailed records of any fees charged with respect to the certified API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

(ii) *Permitted fee – development, deployment, and upgrades*. A Certified API Developer is permitted to charge fees to an API Information Source to recover the costs reasonably incurred by the Certified API Developer to develop, deploy, and upgrade certified API technology.

(iii) *Permitted fee – recovering API usage costs.* A Certified API Developer is permitted to charge fees to an API Information Source related to the use of certified API technology. The fees must be limited to the recovery of incremental costs reasonably incurred by the Certified API Developer when it hosts certified API technology on behalf of the API Information Source.

(iv) *Permitted fee – value-added services*. A Certified API Developer is permitted to charge fees to an API User for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology.

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"
  - All health IT developers under the Program would attest to the "information blocking" Condition of Certification requirement (§ 170.401), while only health IT developers that have health IT certified to the "API" certification criteria (§ 170.315(g)(7) – (10)) would be required to attest to the "API" Condition of Certification and Maintenance requirements (§ 170.404)
- Maintenance of Certification: Health IT developers must attest to ONC-ACBs every six months
  - ONC revised proposed 14-day attestation window to 30 days

Appendix 3: Information Blocking Proposed Rule (March 2019) Comments to ONC
April 2019
Annotated to Show Issues Addressed in Final Rule

(Initial Review—Check marks intended to indicate that the issue was addressed materially in the Final Rule)

Actors and Other Definitions

Actors and Other Definitions: Findings §171.102

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

Information Blocking Practices

Practices: Findings §171.103 and p. 76165

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

Practices: Findings §171.103 and p. 76165

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

Exceptions

Preventing Harm: Findings §171.201

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

Protecting Privacy: Findings §171.202

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

Protecting Security: Findings §171.203

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

Protecting Security: Findings §171.203

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

Recovering Costs Reasonably Incurred: Findings §171.204

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

Recovering Costs Reasonably Incurred: Findings §171.204

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

Recovering Costs Reasonably Incurred: Findings §171.204

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

Infeasible Requests: Findings §171.205

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

Infeasible Requests: Findings §171.205

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

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

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

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

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

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

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

✓ We ask ONC to address an actor's obligation to license intellectual property that they do not yet have and to clarify that inability to honor such a request could be met by the feasibility exception and would not require use of this one as well.

Health IT Performance: Findings §171.207

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

Health IT Performance: Findings §171.207

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

Appendix 4:

Phase 2 Topics: Summary of Discussion and Observations Following Submission of Comments

from

Information Blocking Workgroup Phase 2: Final Report

Guidance to the Community and Implementation Feedback to HHS

Interoperability Matters

1/23/2020

HIE/HIN and Other Key Definitions

Implementation & Compliance Implications/Needs

HIEs/HIN Definitions: HITAC Proposed Revisions

- Definitions too confusing, even for expert likely more confusing in actual practice
- Proposed revisions positive, but still concerns, especially with broad EHI definition
- HITAC proposed revised HIE definition clearer, category overlap removed
  - Unusual to be an HIE if not an HIN.
- Revised HIN definition improved but still too broad, continued use of "or" between criteria underscores broad definition
- Guidance essential for final definitions., including likely scenarios
- Essential to understand how definitions are used by enforcement agencies, such as OIG, ONC, and CMS and whether they have consistent interpretations
- Definitions will be used in other regulations and policies, like TEFCA
- Some broad scope may not matter (e.g., an EHR Developer that is a HIN would have no additional enforcement exposure)
- But, a health plan, not an "actor," could be an HIE or HIN and subject to regulations.
- Will take years for implications of definitions and other elements of enforcement to become clear, through cases and enforcement decisions
  - 25+ years for clarity around fraud and abuse/Stark/Anti-Kickback Statute/ Federal False Claims Act enforcement
- Risk of paralysis in organizational decision-making from policy ambiguity; clarity in definitions essential
- Common theme: definition breadth and overlap has real and practical implications.
- The Workgroup can provide tools and perspectives to help organizations deal with ambiguity

Implementation & Compliance Implications/Needs

HIEs/HIN definitions: Who might be unexpectedly included?

- **Provider organizations**, especially those in ACOs where data sharing essential;
- **Payers** (HIEs/HINs, even under HITAC revision, especially with focus on "agreements");
- "**Individuals**" who "substantially influence" policies (e.g., HIM professionals, privacy officers);
- **Release-of-Information vendors**;
- **Interoperability and interface vendors** and any **organization with "integration" in name or mission**, for example:
  - **Third party integrators** working with health plans and providers
  - Companies providing **technology and technology support for HIEs and HIT developers**;
- **Clinical registries (**many need to use non-standard data elements and terms);
- **Companies that rely on remote data access** for their core functionality, such as analytics and clinical decision support vendor**s**;
- **Standards Development Organizations** (SDOs) and other **organizations that define policies and standards** for the industry; and
- **Digital wellness vendors**

Implementation & Compliance Implications/Needs

HIEs/HIN Definitions

Exceptions

- Unclear which likely most relevant to broad HIE/HIN definitions
- Exceptions proposed by ONC because they promote a public interest/ greater good, not to reduce actor burden and not as safe harbors
- March 2019 CMS interoperability proposed rule has detailed contractual requirements for health plans for interoperability but no exceptions, which plans may need

Provisions likely to be especially challenging or with unique in application to broadly defined HINs or HIEs

- Limits on non-standard technology
- Pricing requirements/exceptions
- Contracting rules (e.g., RAND terms)
- Documentation requirements – many organizations that may be included as HIEs and HINs are less experienced with compliance-related documentation requirements
- "Individuals" defined as HIEs or HINs

Implementation and Compliance Implications/Needs

Interoperability Elements and HIEs/HINs: Organizational Priorities

- Actors and *potential Actors* should think about all issues associated with information blocking compliance
- Plan for the worst case
- Challenging to ensure that smaller clinician practices obtain needed compliance expertise and resources
  - Some clinician practices may be HIE/HIN
- Implementing certain exceptions will require organizational policies and procedures *and* need to integrate these into workflows
  - e.g., "minimum necessary" sub-exception requirements exceed what HIPAA requires
- Think about information blocking implications and obligations for parties with which you do business; threats and opportunities
- Physicians, other clinicians, and provider organizations will continue to view themselves as stewards of patient information and have concerns about vetting apps and API access, despite OIG guidance on HIPAA right of access
- Some organizations may face high volume of requests for information and will have challenges in handling volume
- Ambiguity in definitions and policies will make planning for compliance harder (e.g., actors, EHI vs. PHI, etc.)
- Audits may later show what you thought was best and sufficient effort not good enough, leading to unexpected liability

Information Blocking Practices

Implementation and Compliance Implications and Needs

Are the ONC examples unambiguous and sufficiently specific?

- Examples generally reasonable given underlying statutory and regulatory definitions of information blocking, recognizing areas of ambiguity
- In many ways, examples appear to be catalog of complaints to ONC from stakeholders and can be understood as high priority concerns that will/should motivate enforcement and compliance; there are, however, specific issues per the below points:
  - Recognize/clarify that definition of *Electronic Health Information* (EHI), central to these practices, is not limited to information used for treatment
  - "Promptness" (e.g., for security vetting) is subjective and subject to fact situations
    - General concern if term in a practice example, like "promptness", does not have a corresponding reference in an exception
  - Another issue relates to the ONC practice example for information release, when a provider has capability to do same-day release but takes several days:
    - Such a delay could be reasonable, for example if provider must deal with flawed authorization form, missing key elements in release or a bad signature; and
    - Technical and even process capability may not offset situational specifics

Implementation and Compliance Implications and Needs:

Do you disagree with any of ONCs identified practices?

- Need clarification on whether state or local government would be *Actors (e.g.,* an HIE or HIN), and subject to enforcement
  - If so, several practices would be problematic for government public health agencies
- References to "optional" vs. "required" aspects of standards examples do not align well with how optionality viewed in implementation guides or world of implementers; for example, "optional" generally viewed as optional.
  - Implementation guides usually specific to use case(s)
  - What if optional extension not used exactly as described in the standard or the required part of the standard is not used exactly as prescribed
  - General point: examples and enforcement need more nuanced view of how standards are implemented
- With respect to "[h]ealth system policy requiring consent to exchange EHI for treatment even though not required by law," workgroup members emphasized that multiple federal and state laws at play and important for OIG and ONC to coordinate with SAMSHA (42 CFR Part 2) and state agencies to reduce confusion on how to interpret and harmonize non-HIPAA privacy regulations, which could affect information blocking
  - Is failure of EHR to segregate Part 2 data, which could hinder interoperability (e.g., all data for a patient excluded from exchange), information blocking?
  - Decision on whether to segment at record or data element level could affect ability to exchange data

Implementation and Compliance Implications and Needs:

Do you disagree with any of ONCs identified practices?

- In addition, a vendor may build a capability that a client (e.g., provider or HIE/HIN) chooses to not acquire or implement (e.g., data segmentation)
  - Is provider decision not to acquire or use a capability information blocking, especially when there are cost and ROI considerations for deploying specific capabilities (e.g., the cost to a provider to implement data tagging and segmentation)?
- What is a vendor's obligation to develop and offer capabilities that could enhance interoperability, especially support for certain regulatory requirements?
- Important to recognize that a provider's conservative approach to HIPAA compliance may be well within accepted legal and compliance approaches, especially given concerns with OCR enforcement of HIPAA requirements
  - How will OCR compliance concerns be balanced with OIG/ONC compliance concerns?
- Cures and information blocking regulations may eliminate flexibility in implementation of HIPAA and 42 CFR Part 2 and other privacy and security regulations, some of which have conflicting imperatives (e.g., protect information vs. release information)

Implementation and Compliance Implications and Needs:

Are there examples where "likely" standard especially problematic?

- Concern when "likely" standard in ONC information blocking definition is paired with "knowledge" standards, which are applied differently by type of actor
  - Challenging for HIE (as intermediary) to know which "likely" interpretation to follow; their own or members', which may have different preferences and policies
- HIPAA sometimes authorizes release of information outside of Treatment, Payment or Operations, such as for research via an Institutional Review Board (IRB)
  - Can an outside organization cite its *own IRB* as a rationale to demand exchange?
- "Likely" already coming into play
  - Some companies are demanding immediate information release based on what responding provider views as deficient authorization forms
  - At what point does vetting equal information blocking, especially given "likely" standard?
  - From the Release of Information Vendor perspective, there are times when bad actors submit authorizations for release

Implementation and Compliance Implications and Needs:

Are needed examples missing?

- Vendors charging providers for development or implementation of data segmentation capabilities or other regulatory support
- More definition needed re: “reasonable” costs/fees
- Need examples of "without special effort" and for actor use of third-party developers that may have "all or nothing” consent policies
- Need examples that address *writing* to an EHR as “use” of EHI
  - Writing is much more complex than read access, from a technical, operational and health information management (HIM) perspective
  - Latter issue goes to important role of the HIM function in validating information entered into medical record (e.g., via app or HIE)
- Is an unreadable C-CDA information blocking and what makes a C-CDA unreadable, the vendor implementation or the sending organization’s documentation practices?
- General recognition/concern that information blocking will be “weaponized” via private party negotiations, creating de facto, but private sector, enforcement
- With these and similar examples, ONC and OIG would have extensive discretion on which practices to deem information blocking and select for enforcement

Recovering Costs/RAND Licensing

Implementation and Compliance Implications and Needs

Likely additional documentation burdens for cost-based pricing

- This approach to pricing would be a major departure from current practice
- General concern: could be a burden and have a chilling effect on development, especially for developers and HIEs
  - But likely not for providers or others do not charge for information release
- Level of burden driven in part by extent of “interoperability elements” that are ultimately found subject to information blocking in ONC final rule and needing exception (e.g., API used for data access vs. entire EHR)
- Uncertainty on accounting granularity needed: more granular = greater burden
- Pricing and accounting are under review by organizations given proposed rule
- Required detailed cost accounting could reduce services from developers, etc.
- Uncertainty/concern whether and at what level costs would need to be disclosed to/auditable by regulators and especially data requesters
- “Reasonableness" will depend on facts and circumstances per ONC—who needs to be convinced pricing is reasonable and what documentation needed?

Implementation and Compliance Implications and Needs

Likely additional documentation burdens for cost-based pricing

- May need detailed information on customers and their competitors to ground cost/price documentation in factors like "similarly situated," (e.g., bed size data)
- Will be very challenging to be consistent across all "similarly situated" clients given variability of circumstances, especially for development and implementation costs
- Cost data are proprietary and unclear how this exception addresses that issue
- Potential anti-trust issues for cost disclosure to competitors (e.g., issue of input price disclosure – see https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/dealings-competitors/price-fixing)
- How often will pricing need to be revised as costs are recovered over time?
- How long should cost recovery take, especially as customers leave and arrive and products/services are updated – issue of dynamic vs. static cost structure?
- Need to address cost recovery for non-standard development and implementation, which will be unavoidable in many cases (and need clarity on what costs for "non-standard" implementations are defined/recoverable)
- *To avoid unintended consequences, ONC should consider a higher-level approach focusing on non-discriminatory, transparent and consistent pricing (allowing "apples to apples" comparisons), without need for detailed cost accounting. Cures would permit such an approach as HHS has wide discretion on exceptions (recognizing pricing concerns were major driver for underlying Cures provisions)*

Implementation and Compliance Implications and Needs:

Terms likely to be most problematic (e.g. "reasonable")

- Need very clear definition of terms, especially "reasonable" costs
- Ambiguity around key terms, and broader pricing-related exception issues, could have a chilling effect to business entry and conduct
- *A higher-level focus on pricing transparency can offset need for terms needed for detailed cost accounting approach*

Implementation and Compliance Implications and Needs:

Issues with cost allocation across customers

- Cost allocation across customers will very challenging and need to account for allocation and reflect in prices could radically alter business practices
- Will be impossible for developers to know which customers will want technology under development when pricing is determined as part of go-to-market plans
- Should costs only be allocated over actual customers or over the potential, applicable customer base?
- If development for one client, but potentially applicable for others, need way to price that does not penalize this one client or lead to unsustainable pricing given market dynamics (are cross-subsides prohibited?)
- *Again, a higher-level focus on non-discrimination could obviate the need for detailed cost allocation*

Implementation and Compliance Implications and Needs:

Pricing based on customer size as preferred approach

- Non-profit pricing is partially grounded in expected costs but also reflects need to be able to invest in future projects
- Pricing based on customer/member size (e.g., revenue, employees, number of beds, etc.) common for non-profits (e.g., industry collaboratives and HIEs)
- Customer size can be a reasonable proxy for level of support effort an organization will require
- Pricing by customer size can reflect concern with fairness/ability to pay
- Non-profits would need to invest in more detailed cost and market analyses to rigorously assess role of size as cost proxy and fairness issues

Implementation and Compliance Implications and Needs:

Familiarity with RAND licensing

- There is very low familiarity with RAND licensing among workgroup members and this lack of familiarity is likely widespread across the community of Actors
- While often used by Standards Development Organizations (SDOs) that incorporate third party intellectual property into the standard, it is not clear that RAND is a good fit for terms of licenses to software that developers are selling to customers in a commercial marketplace

Implementation and Compliance Implications and Needs:

Software typically sold via a license that could be subject to RAND

- Much health IT software is sold via a new or existing license
- Compliance will likely increase costs of doing business
- Regulators and actors will need clarity on when cost vs. RAND exception apply and whether any opportunity for strategic choice to rely on one or the other
- It is unclear if the focus of this exception is specific IP (e.g., a code set, patent, or proprietary API) or broader access to all IP associated with interoperability elements in any way
- There is a great need for clarity on scope of the interoperability elements (e.g., API or interface vs entire EHR) to which exception relevant
- The need to respond to licensing requests in 10 business days will be a challenge (similar to need for timely response for “infeasible requests” exception)
- Organizations that primarily license IP could face major business model challenges, with the need for non-discrimination conflicting with complex licensing scenarios
- Patent infringement is subject to treble damages, reinforcing IP licensing complexity

Implementation and Compliance Implications and Needs:

How long will it take to review/revise pricing and licensing?

- For both pricing and contracting, the key issue is when liability for information blocking in context of finalized exceptions begins – the effective date of final rule or will there be a grace period or "learning year"?
- Time needed for review will depend on scope of interoperability elements subject to exceptions – three (3) months is best case even if very narrowly defined but more likely will be a year or more for contract and price review and revision
- If must revisit all agreements and pricing, will be very complex and time consuming – there will be an initial period and additional ongoing review for new ***and*** existing contracts and prices
- For contracting and infeasible exceptions, will need processes to review "timely" or within 10 business days as applicable
- External requests for EHI/interoperability element may come from many sources not specified in the Final Rule and in unanticipated forms and channels
- More generally, will need to establish and document processes for timely handling