Information Blocking Workgroup Meeting #14:
Interoperability Matters

5/8/2020

Workgroup Representatives

Associations and Orgs - health IT community
- Anne Kimbol, HITRUST Alliance
- Jeff Coughlin, HIMSS
- Lauren Riplinger, AHIMA
- Scott Stuewe, DirectTrust
- Samantha Burch, AHA
- Jeff Smith, AMIA
- Matt Reid, AMA
- Mari Savickis, CHIME
- Paul Uhrig, The Commons Project, Co-Chair

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

Health Information Networks and Service Providers
- Angie Bass, Missouri Health Connect
- Dave Cassel, Carequality
- Ammon Fillmore, Indiana Health Information Exchange

Healthcare Providers / Physicians
- David Camitta, CommonSpirit, Co-Chair
- Eric Liederman, Kaiser Permanente

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

Public Health
- John Loonsk, APHL

Developers
- Cherie Holmes-Henry, EHRA/NextGen
- Noah Nuechterlein, Epic
- Josh Mast, Cerner
- Jennifer Stoll, OCHIN
- Micky Tripathi, Arcadia.io
- Rita Bowen, MROCorp

Consultant
- Brian Ahier, MITRE Corporation

Federal Government
- Steve Bounds, SSA

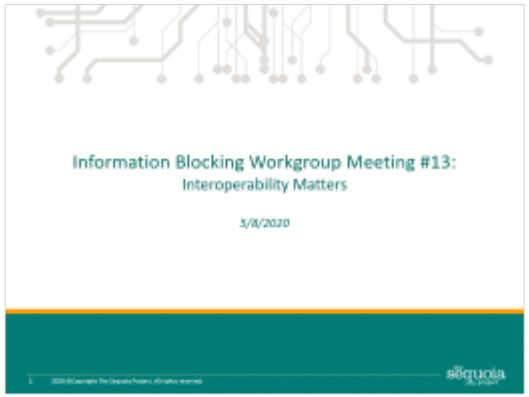
Agenda

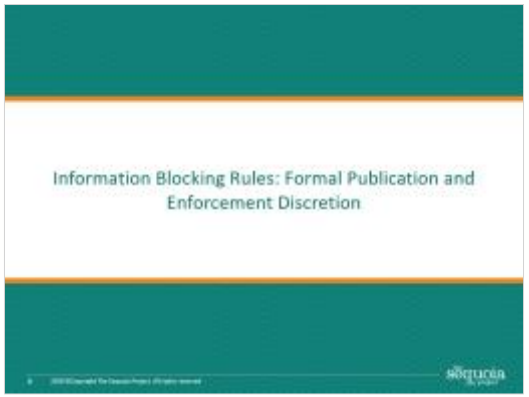
- Welcome and Introductions
- Review of Agenda
- Enforcement Discretion and OIG Proposed Rule
  - Discuss and identify Workgroup comments
- Review and add to priority questions
- Suggestions for Implementation and Compliance Resources
  - Review and discuss April public webinar poll on priorities
- Next Steps
- Closing

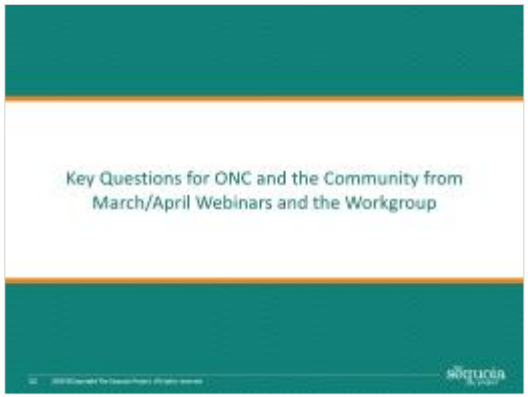
Information Blocking Workgroup: Purpose

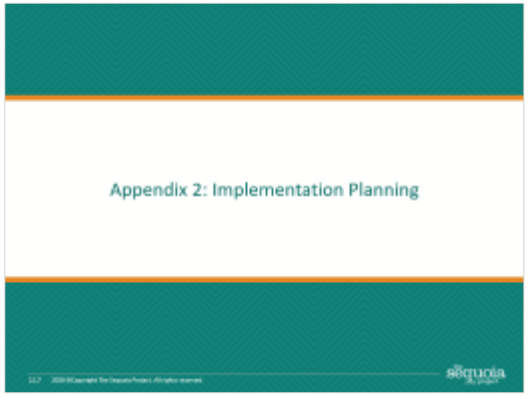
- ✓ Provide input into Sequoia comments to ONC on proposed rule
- ✓ Identify practical, implementation-level implications of proposed and final information blocking rules, which may or may not be consensus positions
- ✓ Facilitate ongoing discussions to clarify information blocking policies and considerations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

Organization of this Deck







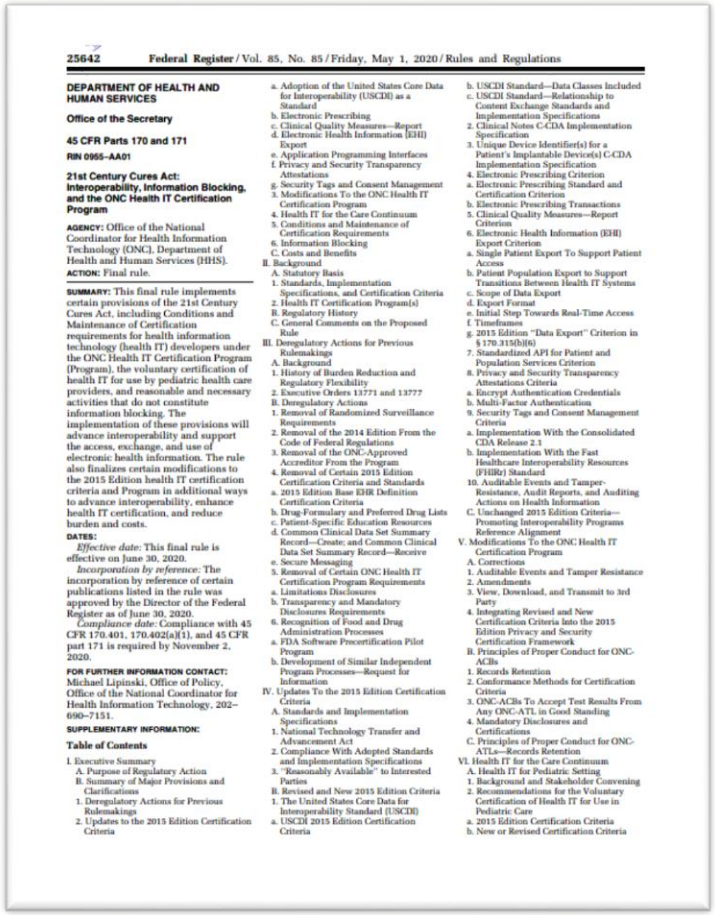


Information Blocking Rules: Formal Publication and Enforcement Discretion

Summary of Actions

- **ONC**
  - Formal publication in the Federal Register: May 1, 2020
  - Announcement of enforcement discretion for certification section of the Final Rule (not information blocking section)
- **OIG**
  - Publication of Proposed Rule addressing information blocking civil monetary penalties: April 24, 2020
  - Includes limited enforcement discretion and delayed effective date
  - Comments sought on some provisions (Information Blocking Workgroup input)
- **CMS**
  - Formal publication in the Federal Register: May 1, 2020
  - Final Rule modified from March display version: ADT CoP pushed out by six months
  - Announcement of enforcement discretion for certain provisions

Enforcement Discretion: ONC



25642 Federal Register / Vol. 85, No. 85 / Friday, May 1, 2020 / Rules and Regulations

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 June 30, 2020.

Incorporation by reference: The incorporation by reference of certain publications listed in the rule was approved by the Director of the Federal Register as of June 30, 2020.

Compliance date: Compliance with 45 CFR 170.401, 170.402(a)(3), and 45 CFR part 171 is required by November 2, 2020.

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

Table of Contents

ONC Final Rule: Enforcement Discretion

- *Pursuant to the 21st Century Cures Act, ONC is tasked with updating the ONC Health IT Certification Program (Program). The ONC Cures Act Final Rule includes new conditions and maintenance of certification requirements that developers certified under the Program are required to meet.*
- *In light of COVID-19, ONC will exercise its discretion in enforcing all new requirements under 45 CFR Part 170* [Certification] *that have compliance dates and timeframes until 3 months after each initial compliance date or timeline identified in the ONC Cures Act Final Rule.*
- *This additional flexibility for development and implementation enables our healthcare system to focus on addressing the COVID-19 pandemic, while still maintaining a trajectory that will advance patients' access to their health information, reduce the cost of care, and improve the quality of care.*

April 21, 2020, https://www.healthit.gov/curesrule/resources/enforcement-discretion. This announcement does not directly affect Part 171—Information Blocking, which is addressed in the OIG Proposed Rule also released on April 21.

ONC Information Blocking and Enforcement Discretion: Timing Updates

- Information Blocking Compliance — 11/2/2020
  - Per May 1 Federal Register publication date
- Conditions of Certification relevant to Information Blocking
  - *Compliance*: Information blocking, APIs, assurances — 11/2/2020
  - *Enforcement:* delayed for 3 months after compliance date — 2/2/2021
  - *Attestation*: (Info blocking, etc.) delayed from 3/31/2021 — 7/30/2021

Proposed Rule and Enforcement Discretion: OIG

OIG Proposed Rule

- Published April 24, 2020
- *Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules*
  Comments due 60 days from publication – June 23, 2020

Federal Register / Vol. 85, No. 80 / Friday, April 24, 2020 / Proposed Rules 22979

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Inspector General

42 CFR Parts 1003 and 1005

RIN 0936–AA09

Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules

AGENCY: Office of Inspector General (OIG), HHS.

ACTION: Proposed rule.

SUMMARY: This proposed rule would amend the civil money penalty (CMP or penalty) rules of the Department of Health and Human Services (HHS or Department) Office of Inspector General (OIG) to: Incorporate new authorities for CMPs, assessments, and exclusions related to HHS grants, contracts, other agreements; incorporate new CMP authorities for information blocking; and increase the maximum penalties for certain CMP violations.

DATES: To ensure consideration, comments must be delivered to the address provided below by no later than 11:59 p.m. Eastern Standard Time on June 23, 2020.

ADDRESSES: In commenting, please reference file code OIG–2605–P. Because of staff and resource limitations, we cannot accept comments by facsimile (fax) transmission. However, you may submit comments using one of three ways (no duplicates, please):

1. *Electronically.* You may submit electronically through the Federal eRulemaking Portal at *http://www.regulations.gov.* (Attachments should be in Microsoft Word, if possible.)

2. *By regular, express, or overnight mail.* You may mail your printed or written submissions to the following address: Aaron S. Zajic, Office of Inspector General, Department of Health and Human Services, Attention: OIG–2605–P, Cohen Building, 330 Independence Avenue SW, Room 5527, Washington, DC 20201.

Please allow sufficient time for mailed comments to be received before the close of the comment period.

3. *By hand or courier.* You may deliver, by hand or courier, before the close of the comment period, your printed or written comments to: Aaron S. Zajic, Office of Inspector General, Department of Health and Human Services, Attention: OIG–2605–P, Cohen Building, 330 Independence Avenue SW, Room 5527, Washington, DC 20201.

Because access to the interior of the Cohen Building is not readily available to persons without Federal Government identification, commenters are encouraged to schedule their delivery with one of our staff members at (202) 619–0335.

Inspection of Public Comments: All comments received before the end of the comment period will be posted on *http://www.regulations.gov* for public viewing. Hard copies will also be available for public inspection at the Office of Inspector General, Department of Health and Human Services, Cohen Building, 330 Independence Avenue SW, Washington, DC 20201, Monday through Friday from 8:30 a.m. to 4 p.m. To schedule an appointment to view public comments, phone (202) 619–0335.

FOR FURTHER INFORMATION CONTACT: Robert Penezic at (202) 205–3211, Office of Counsel to the Inspector General.

SUPPLEMENTARY INFORMATION:

I. Executive Summary:

A. Purpose and Need for Regulatory Action

This proposed rule seeks to address three issues: (1) The amendment of the Civil Monetary Penalties Law (CMPL), 42 U.S.C. 1320a–7a, by the 21st Century Cures Act (Cures Act), Public Law 114–255, sec. 5003, authorizing HHS to impose CMPs, assessments, and exclusions upon individuals and entities that engage in fraud and other misconduct related to HHS grants, contracts, and other agreements (42 U.S.C. 1320a–7a(o)–(s)); (2) the amendment of the Public Health Service Act (PHSA), 42 U.S.C. 300jj–52, by the Cures Act authorizing OIG to investigate claims of information blocking and providing the Secretary of HHS (Secretary) authority to impose CMPs for information blocking; and (3) the increase in penalty amounts in the CMPL effected by the Bipartisan Budget Act of 2018 (BBA 2018), Public Law 115–123. Each of these issues is discussed further below.

First, this proposed rule would modify 42 CFR parts 1003 and 1005 to add HHS's new authority related to fraud and other misconduct involving grants, contracts, and other agreements into the existing regulatory framework for the imposition and appeal of CMPs, assessments, and exclusions. The additions would: (1) Expressly enumerate in the regulation, HHS's grant, contract, and other agreement fraud and misconduct CMPL authority; and (2) give individuals and entities sanctioned for fraud and other misconduct related to HHS grants, contracts, and other agreements, the same procedural and appeal rights that currently exist under 42 CFR parts 1003 and 1005 for those sanctioned under the CMPL and other statutes for fraud and other misconduct related to, among other things, the Federal health care programs. We propose to codify these new authorities and their corresponding sanctions in the regulations at §§ 1003.110, 1003.130, 1003.140, 1003.700, 1003.710, 1003.720, 1003.1550, 1003.1580, and 1005.1.

Second, Section 4004 of the Cures Act added sec. 3022 to the PHSA, 42 U.S.C. 300jj–52, which, among other provisions, provides OIG the authority to investigate claims of information blocking and authorizes the Secretary to impose CMPs against a defined set of individuals and entities that OIG determines committed information blocking. Investigating and taking enforcement action against individuals and entities that engage in information blocking is consistent with OIG's history of investigating serious misconduct that impacts HHS programs and beneficiaries. Information blocking can pose a threat to patient safety and undermine efforts by providers, payers, and others to make our health system more efficient and effective. Addressing the negative effects of information blocking is consistent with OIG's mission to protect the integrity of HHS programs, as well as the health and welfare of program beneficiaries.

We propose to implement 3022(b)(2)(C), which requires information blocking CMPs to follow the procedures of sec. 1128A of the Act. Specifically, the proposed rule would add the information blocking CMP authority to the existing regulatory framework for the imposition and appeal of CMPs, assessments, and exclusions (42 CFR parts 1003 and 1005), pursuant to the PHSA sec. 3022(b)(2)(C) (42 U.S.C. 300jj–52(b)(2)(C)). The proposed modifications would give individuals and entities subject to CMPs for information blocking the same procedural and appeal rights that currently exist under 42 CFR parts 1003 and 1005. We propose to codify this new information blocking authority at §§ 1003.1400, 1003.1410, and 1003.1420. The proposed rule also explains OIG's anticipated approach to enforcement and coordination within HHS to implement the information blocking authorities.

The Office of the National Coordinator for Health Information Technology (ONC) has finalized the

April 21, 2020. https://oig.hhs.gov/newsroom/news-releases/2020/infoblocking.asp

Legal Authority Cited in OIG Proposed Rule

- The Cures Act amended the Public Health Services Act (PHSA) o authorize the HHS Office of Inspector General (OIG) to investigate claims of information blocking and authorizes the HHS Secretary to impose Civil Money Penalties (CMPs) for information blocking
- OIG notes that information blocking can pose a threat to patient safety and undermine efforts to make health system more efficient and effective
- OIG specifically incorporates the ONC Final Rule as the legal basis for imposing CMPs and determining the amount of a CMP
- The OIG NPRM also addresses HHS expanded authority to impose CMPs, assessments and exclusion for false information/claims for HHS grants, contracts and other agreements (beyond scope of this presentation)

CMP Applicability

- CMPs can be imposed on developers or other entities offering certified health IT, health information exchanges or networks
- Healthcare providers are not subject to CMPs unless also an HIE/HIN (or developer of certified health IT)
- Providers that OIG determines are information blocking will be referred to appropriate agency to be subject to disincentives under applicable law
  - e.g., HHS OCR for HIPAA or CMS re: incentive program attestations

OIG Investigations

- OIG has discretion on which complaints to investigate
- OIG will use its 35-year institutional experience to decide which complaints to investigate—introduces considerable uncertainty
- OIG will select cases to investigate consistent with OIG's priorities and expects to focus on cases that:
  - Caused or could cause patient harm
  - Significantly impacted a provider's ability to provide patient care
  - Persist over a long duration
  - Cause financial loss to Federal health care programs, other government or private entities
  - Actual knowledge by the Actor

The Role of Intent

- Information blocking violation requires intent
  - Actual knowledge for providers
  - Actual or implied knowledge for all others
- OIG lacks authority to pursue information blocking CMPs against Actors who it determines did not have requisite intent
  - **OIG will not bring enforcement actions against Actors that make "innocent mistakes"**
- Every allegation will be evaluated based on the facts and circumstances unique to that case

CMP Penalty Determination: Comments Sought

- OIG may impose a CMP of up to $1 million “per violation”
- OIG will determine the amount of the CMP based on:
  - The nature and extent of the information blocking
  - The harm resulting from the information blocking
  - The number of patients affected
  - The number of providers affected
  - The duration of the information blocking calculated as the number of days the blocking persists
- **OIG seeks comment on additional aggravating or mitigating factors**

OIG Proposed Rule: Enforcement Timing

- *"OIG will not begin enforcing the information blocking CMPs until the OIG CMP information blocking regulations are effective. We are proposing that the **effective date of these regulations be 60 days from the date of publication** of our final rule.*
  - *We are **also considering an alternative proposal for the effective date** of subpart N described in detail later in this preamble."*
- *"The goal in exercising our enforcement discretion is to **provide individuals and entities that are taking necessary steps to comply with the ONC Final Rule with time to do so while putting the industry on notice** that penalties will apply to information blocking conduct within a reasonable time."*

OIG Proposed Rule: Enforcement Timing Details

- ONC notes that section 3022(b) of the PHSA is self-implementing and the only explicit timing limitation of the information blocking provision is in section 3022(a)(4) of the PHSA
- OIG will exercise enforcement discretion to only impose CMPs against Actors who have engaged in information blocking **after effective date** of its final rule
  - **Conduct prior to effective date of OIG final rule will not be subject to information blocking CMPs**
  - The ONC Final Rule had also suggested that conduct before the compliance date of the information blocking provisions of the ONC final rule would not be subject to CMPs

OIG Proposed Rule: Enforcement Timing Details

- Individuals and entities subject to the information blocking regulations must comply with the **ONC Final Rule** as of the compliance date the Information blocking provisions of that rule
  - *"The period between the compliance date of the ONC Final Rule [11/1/2020] and the proposed start of OIG's information blocking enforcement will provide individuals and entities with time to come into compliance with the ONC Final Rule with added certainty that practices during that period will not be subject to penalties."*
  - *"We believe the proposed effective date of 60 days after publication of the OIG final rule provides a reasonable amount of time for individuals and entities to come into compliance with ONC's Final Rule."*
- **Compliance date** of the ONC Final Rule appears unchanged by **ONC** enforcement discretion, which only applies to certification issues

Enforcement Timing—Alternate Proposal: Comments Sought

- OIG is considering for the final rule an alternative proposal for the effective date to apply only to subpart N of part 1003, which would also affect the start of OIG's information blocking enforcement
  - The alternative proposal would establish a specific date that OIG's information blocking CMP regulations would be effective; OIG is considering October 1, 2020
  - ONC seeks *"to provide entities a time certain that OIG enforcement will begin."*
  - *"As discussed above, individuals and entities are legally subject to the information blocking regulations and must comply with those rules as of the compliance date of ONC's Final Rule finalized at 45 CFR 171.101(b)."*
  - *"This alternative proposal would provide a definite period to these individuals and entities to continue their compliance efforts with the ONC Final Rule with the knowledge that their conduct would not be subject to OIG enforcement until October 1, 2020. OIG believes that this time frame would be more than adequate for actors to implement necessary changes to align with ONC's Final Rule. At a minimum, enforcement would not begin until the compliance date of the ONC Final Rule finalized at 45 CFR 171.101(b)."*
  - *"[A] specific date to target may assist in the execution and timing of amending agreements, issuing updates, or other actions needed to comply with the ONC Final Rule. We recognize that proposing a specific effective date would require OIG to complete the final rulemaking process before this proposed specific date. We have considered that factor and believe this alternative proposal allows time for that process."*
- **ONC solicits comment on these proposed approaches:**
  - **It is considering alternative effective dates sooner or later than October 1, 2020 and seeks comments on potential dates and explanations about why parties would need a longer or shorter time period to come into compliance with the ONC Final Rule**

OIG Regulatory and Enforcement Approach: Comments Sought

- OIG investigations of information blocking will use ONC's regulatory definitions and exceptions to assess conduct by developers of certified technology, entities offering certified health IT, HINs/HIEs and providers
- ONC Final Rule provisions are incorporated by reference in OIG's proposed regulations
- Under the proposal to incorporate information blocking CMP into 42 CFR part 1003, any CMP determination based on an investigation of information blocking would be subject to CMP procedures and appeal process in parts 1003 and 1005
- **ONC solicits comment, for purposes of a final rule, on the proposed incorporation of the information blocking regulations into 42 CFR part 1003, and the proposed application of the existing CMP procedures and appeal process in parts 1003 and 1005 to the information blocking CMPs**

Maximum Penalties: Comments Sought

- OIG proposes to add a new § 1003.1410 to codify the maximum penalty OIG can impose per violation of the information blocking provisions
  - PHSA sec. 3022(b)(2)(A) authorizes a maximum penalty of $1,000,000 per violation and proposed regulatory language reflects this maximum
  - **OIG solicits comments on this proposed regulatory language**
- The proposed rule would define "violation" as each "practice" that constitutes "information blocking," using definitions in the ONC Final Rule
- To explain the intent of the proposed definition of "violation" and illustrate how OIG would determine what constitutes a single violation or multiple violations, OIG notes that ONC provides hypothetical examples of conduct that would meet the definition of information blocking

OIG Examples of a Single Violation

- A health care provider notifies its health IT developer of its intent to switch to another EHR system and requests a complete electronic export of its patients' EHI via the capability certified to in 45 CFR § 170.315(b)(10). The developer refuses to export any EHI without charging a fee. **The refusal to export EHI without charging this fee would constitute a single violation.**
- A health IT developer (D1) connects to a health IT developer of certified health IT (D2) using a certified API. D2 decides to disable D1's ability to exchange information using the certified API. D1 requests EHI through the API for **one patient** of a health care provider for treatment. As a result of D2 disabling D1's access to the API, D1 receives an **automated denial of the request**. **This would be considered a single violation.** [Note the focus on a refusal for a single patient by another developer.]

OIG Examples of a Single Violation: Comments Sought

- For these examples, the facts or circumstances could affect the penalty amount but would not likely result in determining that there were multiple violations
  - However, when investigating information blocking, OIG will assess facts and circumstances on a case-by-case basis, which may lead to determination of multiple violations
- In the first example, the number of patients affected by the health IT developer's information blocking practice is a factor OIG would consider when determining the penalty amount
- For determining the number of violations, the important fact would be that the developer engaged in one practice (charging a fee to the health care provider to perform an export of electronic health information for the purposes of switching health IT) that meets the elements of the information blocking definition in 45 CFR 171.103(a)
  - Although several patients might be affected by the health IT developer's practice of information blocking, the health IT developer only engaged in one practice in response to the request from the provider. Therefore, under the proposed rule, the fact scenario in this example would constitute only one violation
- **ONC solicits comments, for purposes of the final rule, on the examples of a single violation and what constitutes a single violation**

OIG Examples of Multiple Violations

- A developer's software license agreement with one customer prohibits the customer from disclosing to its IT contractors certain technical interoperability information (i.e. Interoperability elements), without which the customer and the IT contractors cannot access and convert EHI for use in other applications. The developer also chooses to perform maintenance on the health IT that it licenses to the customer at the most inopportune times because the customer has indicated its intention to switch its health IT to that of the developer's competitor. **For this specific circumstance, one violation would be the contractual prohibition on disclosure of certain technical interoperability information and the second violation would be performing maintenance on the health IT in a discriminatory fashion. Each violation would be subject to a separate penalty.** [Note the problematic contract provision as a violation.]
- A developer requires vetting of third-party applications before the applications can access the developer's product. The developer denies applications based on the functionality of the application. **There are multiple violations based on each instance the health IT developer vets a third-party application because each practice is separate and based on the specific functionality of each application. Each of the violations in this specific scenario would be subject to a penalty.**

OIG Examples of Multiple Violations: Comments Sought

- For the examples illustrating multiple violations, ONC notes that important facts, in determining number of violations, are the **discrete practices** that each meet the elements of information blocking definition
- In the first example, the developer engages in two separate practices: (1) prohibiting disclosure of certain technical interoperability information and (2) performing maintenance on the health IT in a discriminatory fashion
  - Each practice would meet the definition of information blocking separately and therefore, the first example is a two-violation scenario
- In the second example, the health IT developer vets each third-party application separately and makes a separate decision for each application.
  - For each denial of access to EHI based on discriminatory vetting, there is a practice that meets the definition of information blocking and thus, each denial of access would be a separate violation
- **ONC solicits comments on the proposed definition of "violation"**

Proposed Regulatory Text

Subpart N—CMPs for Information Blocking

§ 1003.1400 Basis for civil money penalties.

The OIG may impose a civil money penalty against any individual or entity described in 45 CFR 171.103(b) that commits information blocking, as defined in 45 CFR part 171.

§ 1003.1410 Amount of penalties.

(a) The OIG may impose a penalty of not more than $1,000,000 per violation.

(b) For this subpart, *violation* means a practice, as defined in 45 CFR 171.102, that constitutes information

blocking, as defined in 45 CFR part 171.

§ 1003.1420 Determinations regarding the amount of penalties.

In considering the factors listed in § 1003.140, the OIG shall take into account—

(a) The nature and extent of the information blocking; and

(b) The harm resulting from such information blocking, including, where applicable--

(1) The number of patients affected;

(2) The number of providers affected; and

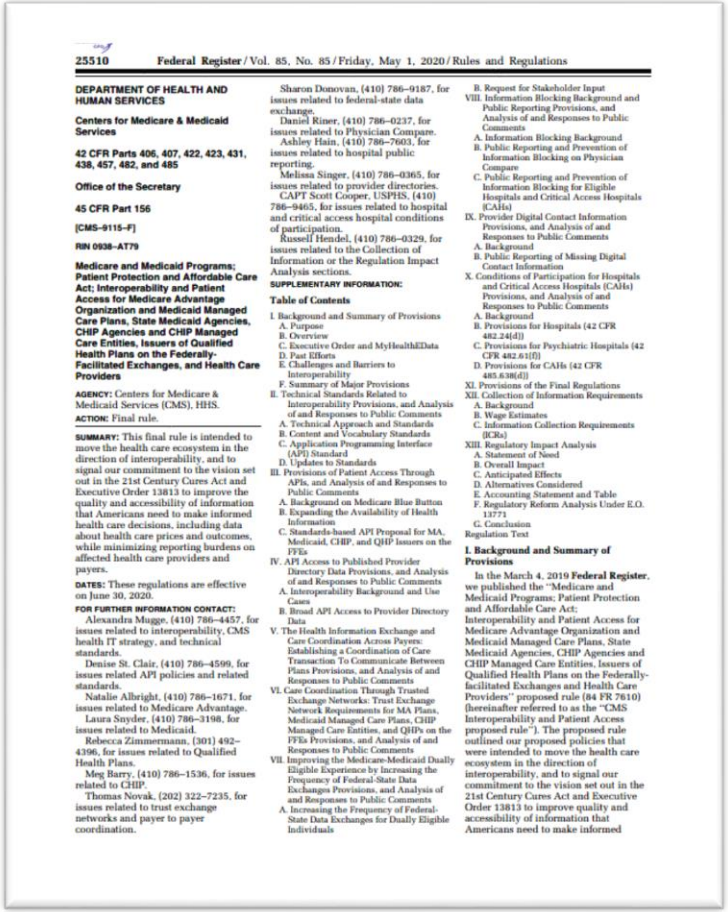
(3) The number of days the information blocking persisted.

OIG Proposed Rule: Details for Comments

- Published April 24, 2020
- DEPARTMENT OF HEALTH AND HUMAN SERVICES
  Office of Inspector General
  42 CFR Parts 1003 and 1005
  RIN 0936-AA09
  Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules
  AGENCY: Office of Inspector General (OIG), HHS.
  ACTION: Proposed rule.
- **Comments due 60 days from publication – June 23, 2020**
  - File code: OIG-2605-P
- Addresses, with two other issues, "the amendment of the Public Health Service Act (PHSA), 42 U.S.C. 300jj-52, by the Cures Act authorizing OIG to investigate claims of information blocking and providing the Secretary of HHS (Secretary) authority to impose CMPs for information blocking"

April 21, 2020. https://oig.hhs.gov/newsroom/news-releases/2020/infoblocking.asp

Enforcement Discretion: CMS



25510 Federal Register / Vol. 85, No. 85 / Friday, May 1, 2020 / Rules and Regulations

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

42 CFR Parts 406, 407, 422, 423, 431, 438, 457, 482, and 485

Office of the Secretary

45 CFR Part 156

[CMS–9115–F]

RIN 0938–AT79

Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers

AGENCY: Centers for Medicare & Medicaid Services (CMS), HHS.

ACTION: Final rule.

SUMMARY: This final rule is intended to move the health care ecosystem in the direction of interoperability, and to signal our commitment to the vision set out in the 21st Century Cures Act and Executive Order 13813 to improve the quality and accessibility of information that Americans need to make informed health care decisions, including data about health care prices and outcomes, while minimizing reporting burdens on affected health care providers and payers.

DATES: These regulations are effective on June 30, 2020.

FOR FURTHER INFORMATION CONTACT:
Alexandra Mugge, (410) 786–4457, for issues related to interoperability, CMS health IT strategy, and technical standards.
Denise St. Clair, (410) 786–4599, for issues related API policies and related standards.
Natalie Albright, (410) 786–1671, for issues related to Medicare Advantage.
Laura Snyder, (410) 786–3198, for issues related to Medicaid.
Rebecca Zimmermann, (301) 492–4396, for issues related to Qualified Health Plans.
Meg Barry, (410) 786–1536, for issues related to CHIP.
Thomas Novak, (202) 322–7235, for issues related to trust exchange networks and payer to payer coordination.
Sharon Donovan, (410) 786–9187, for issues related to federal-state data exchange.
Daniel Riner, (410) 786–0237, for issues related to Physician Compare.
Ashley Hain, (410) 786–7603, for issues related to hospital public reporting.
Melissa Singer, (410) 786–0365, for issues related to provider directories.
CAPT Scott Cooper, USPHS, (410) 786–9465, for issues related to hospital and critical access hospital conditions of participation.
Russell Hendel, (410) 786–0329, for issues related to the Collection of Information or the Regulation Impact Analysis sections.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Background and Summary of Provisions

In the March 4, 2019 **Federal Register**, we published the "Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-facilitated Exchanges and Health Care Providers" proposed rule (84 FR 7610) (hereinafter referred to as the "CMS Interoperability and Patient Access proposed rule"). The proposed rule outlined our proposed policies that were intended to move the health care ecosystem in the direction of interoperability, and to signal our commitment to the vision set out in the 21st Century Cures Act and Executive Order 13813 to improve quality and accessibility of information that Americans need to make informed

Enforcement Discretion: CMS (4/21/2020)

Current (Per Published Final Rule)	Enforcement Discretion
• Patient Access API (including Exchange QHPs) (*January 1, 2021*)	• To July 1, 2021
• Provider Directory API (*January 1, 2021*)	• To July 1, 2021
• Condition of Participation Admission, Discharge, and Transfer Event Notifications (S*pring 2021*)	• Note: In the Final Rule published May 1, 2020, CMS had moved ADT COP from 6 months (in initial display copy of the rule) to 12 months after Final Rule publication • **All other dates remain in force**

April 21, 2020. https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

Key Questions for ONC and the Community from March/April Webinars and the Workgroup

Key Questions from Webinars

Who do the Rules Apply To: Actors: HIE/HIN, Payors, etc.?

- Do Public Health programs meet the definition of an HIE/HIN and therefore become subject to the information blocking requirements?
  - Some programs (e.g., immunization registries) collect data from multiple sources (multiple provider organizations) and share with providers. Does this qualify as facilitating exchange by more than two entities?
- I'd like to hear if Public Health programs meet the definition of either an HIE or an HIN and are subject to the requirements of information blocking. Some programs, such as immunization registries, do collect data from multiple sources and share it. (4/17)

- How does this Rule apply to Payers (e.g., health insurance companies)?
- Does information blocking apply to payers as well as providers? (4/17)
- Generally hoping to learn more about how payers are impacted. (4/17)

- How do the ONC information blocking rules apply (and to be implemented by) entities that may not have a direct patient/provider relationship, such as a laboratory or consulting physician?

- Do the requirements apply to only entities with data subject to HIPAA or data outside of HIPAA (that may have been disclosed by a HIPAA-covered entity)?

Key Questions from Webinars

Who do the Rules Apply To: Actors: HIE/HIN, Payors, etc.?

- Clearinghouses exchange far more data than just claims. Does the exclusion of clearinghouses include any information exchanged by health care clearinghouses, or just claim data?
- How does the rule apply to multi-specialty physician groups? (4/17)
- Please address examples of entities meeting the new definition of HIE/HIN. (4/17)
- How can HIEs/HINs be held to a higher standard that the providers? They are the Covered Entities, we are Business Associates, and we can only share data in accordance with our contracts and BAA terms. (4/17)
- I am interested in HIE requirements and how HIE supports new rulings. (4/17)
- I am curious about what must an HIN/HIE do to be compliant in ways of sharing data - CCDA or FHIR with data elements specified in USCDI is my understanding. (4/17)
- It is clear that HIN/HIEs are actors in Information Blocking. However, most do not do Certification. If they do not do Certification, must they still support USCDI? In one or both of FHIR and CCDA? Or in "some standard format"? (4/17)

Key Questions from Webinars

EHI and USCDI

- If the USCDI doesn't have to be implemented for 24 months after publication of the Final Rule, what does it mean that information blocking scope is restricted to EHI (defined as USCDI data elements) for the first 24 months after publication of the Final Rule (e.g. if provenance isn't implemented until the 24 months, is it information blocking if provenance isn't implemented at month 6?
- In the Final Rule (beginning on page 59 and again on page 101), with respect to the API requirements – it appears that six months after the publication of the final rule, systems much be able to access and exchange codes from within the USCDI definition. The timeline for certification compliance with the USCDI definition is 24 months from the date of publication.
  Do the API requirements mandate that ALL USCDI codes must be available to access and exchange at the six-month compliance date or only that all codes available to access and exchange at that time must be from within the USCDI definition? Additionally, if the interpretation is that all USCDI codes must be available at the six-month date of compliance, should developers be seeking a Content and Matter exception until they complete the full transition to the USCDI specifications. (4/17)

Key Questions from Webinars

EHI and USCDI

- How much of legacy EHR data is a hospital required to provide through APIs if only some discrete data were converted to the current EHR and the rest is in PDF format (chart export from the old EHR). We're assuming all under USCDI, but would like opinions (4/17)
- What are the designated record sets per HIPAA that are required to be shared by providers and other actors at 24 months after publication? What are technologies that must be used to share this greatly expanded set of data? (4/17)|
- Information blocking will take effect 6 months after publication. Is the expectation to exchange using the USCDI as the minimum requirement? Is the Common Clinical Data Set (CCDS) still viable until it is ready? (4/17)

Standards

- When will FHIR 4 be supported? Does this include everyone connected? Will real time transactions be supported? Will research queries be supported (no patient specific)? (4/17)

Access, Exchange, Use

- Please explain “write” access requirements on API information blocking? Isn’t it “read-only”?
- What is impact for HIEs that do not have patient access to portal re: API requirements?

Key Questions from Webinars

Is it Information Blocking?

- If a state HIE asked the hospitals in that state to participate (and offered to cover associated expenses), and the hospitals declined, would this action by the hospitals be considered information blocking?
- If a group of providers refused to permit an HIE to provide de-identified data for evaluation of a program or service of a provider, does that refusal constitute data blocking?
- If providers refused to permit an HIE to send batch downloads of patient information for purposes of quality measurement, would that be data blocking?
- If organizations refuse to do setup for Summary of Care measures, is that information blocking?
- Some Hospitals are only sending ADTs and not sending other data types to their HIEs, will this be considered as information blocking?

Key Questions from Webinars

Is it Information Blocking?

- Would a clinical registry operated by a third-party, such as a health care quality collaborative operating a clinical registry and offering quality measurement and reporting services to provider entities (i.e., healthcare operations), generally not be considered an HIN/HIE and fit the criteria of bilateral exchange?
- How do we expect requests to come through from third party developers and from patients? (4/17)
- I need proper understanding of information blocking and how that affects HIE's and more detail around the exceptions. (4/17)
- Given a feasible request for EHI where no exception is provided- could you comment on what is expected to be a reasonable timeframe for an actor to exchange requested EHI? At what point could an actor be capable of info blocking if the request is delayed? (4/17)

Key Questions from Webinars

Privacy and Security Exceptions

- How does 2nd bullet on Slide 31 (of the March webinar) jibe with the Privacy Exception Precondition not satisfied: If an actor is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing access, exchange, or use?
- Could state laws conflict with information blocking objectives, and if so, how should HIEs properly document that certain sensitive data (i.e. HIV, SUD) must be blocked to remain compliant with either state laws or contractual agreements?
- Can you speak specifically to the exchange of sensitive data, including both behavioral health and substance use data? (4/17)

Preventing Harm Exception

- ONC: Does the decision to restrict notes made at time of their creation count as having been determined on an individual basis by a licensed provider in historical context? [Many departments and specialties restrict access to notes created in certain circumstances (e.g., just viewable by the author or a department)]

Key Questions from Webinars

Infeasibility Exception

- ONC: can we use the infeasibility exception because it was infeasible when we intended to be building implementation and compliance plans, although “now” it would appear technically feasible?

Fee Exception

- Why is the language in 171.301(b)(2) regarding fees being prohibited for electronic access of an individual's EHI by "another person or entity designated by the individual" not in conflict with the recent DC District Court decision on the Ciox v. Azar case related to fees charged to third parties it which an individual directs his/her health information be transmitted?
  - The nuance may be the definition of electronic access in Part 171: to mean an internet-based method that makes the EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request. If this is not the type of access requested by the individual, the HIPAA fee decision of the court may apply.
  - If I was a lawyer that did malpractice cases, I would procure a consumer-facing app that uses FHIR R4 and provide that to my client to access the client's EHI.
- Is cost considered in the blocking of interoperability? (4/17)
- Will cost of integration be considered in data blocking definition? (4/17)

Discussion/Questions from April 2020 Workgroup

Fees and Licensing Exceptions

- ONC: ONC outlines that the 10-day and 30-day timelines required to meet the licensing exception are triggered by receipt of a request for license or use of EHI (p. 976) even when the requestor does not understand the need for a license. What needs to occur within the 30-day timeline? Do negotiations need to be completed within the 30-day timeframe?
  - A 30-day timeline from the point of request to complete negotiations does not seem realistic for many scenarios.
- The Fees exception contains a condition that requires HIT Developers to comply with the Conditions of Certification related to EHI Export and APIs "for all practices and at all relevant times." The language seems to indicate that an HIT Developer would need to comply with Condition of Certification requirements for non-certified functionality.
  - ONC: Is the intent for Developers of certified health IT to comply with these conditions at all times for all certified modules, the wording is not clear and needs to be clarified.
    - Staff: Some Conditions of Certification seem to be limited to certified health IT (e.g., for certified APIs) and others focus on the Actor's organization (e.g., information blocking).

Discussion/Questions from April 2020 Workgroup

Content and Manner Exception

- ONC: If an Actor can respond to the request in "any manner requested" and the requested manner is one of the hierarchy of response options if "any manner" is not met, does the use of such an approach (e.g., ONC certification standard) mean that Fee and/or Licensing exceptions must be used?
- ONC: If an Actor is working through the Content and Manner exception and moves to alternative manners and parties still do not reach agreement, does the process end?
  - Could then turn to the Infeasibility exception, per ONC
  - But, there is a potential timing issue with that approach. The Infeasibility exception requires the Actor to respond to the request within 10-business days of the request outlining the reasons for claiming the request is infeasible and by the time an Actor completes stepping through the Content and Manner exception it could very likely already be past the 10-day requirement.
- ONC: During the period before the updated API and USCDI certification requirements are required, should the requested functionality that aligns with the 2015 CEHRT Cures Update requirements be treated as complying with the manner requested under the Content and Manner exception or as complying with the alternative manner Certification/nationally adopted standards requirements? In addition, is it acceptable to inform the requestor that the requested functionality is under development and outline the expected timeline as part of the agreement under the Content and Manner exception?

Discussion/Questions from April 2020 Workgroup

Content and Manner Exception

- Under the Content and Manner Exception if a request is fulfilled in the manner requested, the actor need not comply with the Fees and Licensing exceptions but fulfilling a request in an alternative manner does require compliance with the Fee and Licensing exceptions.
  - The way this exception is worded could potentially allow for scenarios in which two requests are received, ultimately fulfilled in the same manner, but one would comply with the Fees and Licensing Exception and one would not. The example scenario would play out in years when the 2015 Edition Cures-related Updates are in effect and two requestors (requestor 1 and requestor 2) make similar requests to an Actor.
    - Requestor 1 makes a request for a standards-based API functionality using FHIR R4 for USCDI information and requestor 2 makes a request for a proprietary API to access USCDI. The Actor fulfills request 1 in the manner requested and does not need to comply with the Fees or Licensing exceptions. The Actor claims an inability to meet request 2 on technical reasons and moves to offer an alternative manner which is API access using FHIR R4, and the offer is accepted by the requestor. When the Actor completes request 2 it must meet the Fees and Licensing exceptions even though it is supplying the same functionality as in request 1.
  - ONC: Is this analysis correct and should this disparity be addressed or eliminated?
- ONC: Does the Content and Manner exception allow for development time or agreement to deliver functionality after additional development? It is not clearly stated in the preamble or the regulation. There is mention of fulfilling request without undue delay; development time would add a delay, but would it be undue?

Discussion/Questions from April 2020 Workgroup

Content and Manner Exception

- ONC: If an actor works through the process of the Content and Manner exception and cannot reach an agreement on the manner requested or any of the alternative manners, does the actor have to claim Infeasibility or is lack of agreement enough? The rule seems to hint that the actor would claim Infeasibility however there is a potential timing issue with that. The infeasibility exception requires the actor to respond to the request within 10-business days of the request outlining the reasons for claiming the request is infeasible and by the time an actor completes stepping through the Content and Manner exception it could very likely already be past the 10-day requirement.

Key Questions from Webinars

Implementation and Enforcement Dates

- When is the final ruling on this going to be done? (4/17)
- Does it seem likely that the Rules will be delayed being published in the Federal Register and therefore the timeline for industry implementation and adherence may also be delayed? (4/17)
- Are there any changes to the critical deadlines given competing resources due to COVID-19?
- Has any consideration been given to pushing out any dates due to COVID-19 activities?

- My understanding from the briefing at the March HITAC is that the compliance date for information blocking per se is not tied to when the OIG's enforcement and CMP rule is final.
  - The actual enforcement of the information blocking provision and CMPs may be delayed and the rule indicates enforcement would be no earlier than the 6-month compliance date. It was not very clear in the rule and ONC should clarify this in an FAQ.
  - One could say a compliance date that has no enforcement in effect is equivalent to a compliance delay. For a health care provider, getting started on coming into compliance with the Information Blocking provision sooner rather than later is better now that the rule is out.
- When will the penalties be in effect? (4/17)
- Please further discuss issues associated with enforcement (ONC & OCR) especially related to Individual Rights. (4/17)

Key Questions from Webinars

Business Associate Agreements (BAAs)

- What wording should we pay attention to in our business associate agreements? What are red flags? (4/17)

Organizational Policies and Contracts

- What type of policies do you recommend having in place to address Information Blocking for EHRs? (4/17)
- I'm interested in learning about Sequoia's thoughts on how organizations might go about updating existing health IT contracts to ensure compliance with information blocking exceptions. (4/17)

General Suggestions

- Would love to hear real stories, initial experiences, if any, about the implementation of this policy.
- Interested in knowing what provider organizations need to be aware of, related to information blocking. (4/17)

Implementation and Compliance Resources and Other Next Steps

Resources for the Community

Polling from April Public Webinar

- **82% - Compliance guides**
- **79% - Implementation tools and checklists**
- 59% - Facilitating ONC presentations and Q&A
- 55% - Additional Sequoia Project webinars
- 36% - Opportunities for moderated industry discussion

Workgroup Suggestions

Interoperability Matters

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

Appendix 1: Final Rule Materials from the March and April 2020 Meetings

Key Workgroup Discussion Points: March and April 2020

Discussion from March 2020 Meeting

ONC NPRM public comment themes and responses

- ONC did not clarify/or better define “likely”.

Major Changes from NPRM

- Given federal government focus on COVID-19, we cannot expect the Final Rule will be published in the Federal Register any time soon. A delay in publication could be one way to slow down implementation.

Revised Definitions

- HIE/HIN definition: A lot rides on what is meant by “unaffiliated”; are contracted providers affiliated? Note there is some discussion of affiliated in the preamble, including examples (e.g. where a provider organization controls an HIE.).

Finalized Exceptions

- The shift to using case-by-case analysis if an exception is not met, intersects with “know or should have known” – which impacts providers, but not HIT developers.

Discussion from March 2020 Meeting

Preventing Harm Exception

- There is a lot of debate in the provider world about including imaging results and pathology results, not just lab results. Psychiatric notes are another concern. These issues need sorting out.
- Issue for future discussion: Many departments and specialties restrict access to notes created in certain circumstances (e.g., just viewable by the author or a department)
- *Question for ONC: Does the decision to restrict notes made at time of their creation count as having been determined on an individual basis by a licensed provider in historical context?*

Infeasibility Exception

- Public health emergency: can we invoke this exception during/after the current emergency and push back the 6-month compliance deadline of the Final Rule?
- There is a low likelihood of enforcement actions given current federally declared disaster.

Discussion from March 2020 Meeting

Content and Manner Exception

- Fee requirements will need closer consideration.
- Is there a loophole where parties who use an intermediary can block information sharing? There is a hierarchy test to assess whether it matters:
  - If you are in middle of bilateral exchange as an intermediary, you are not an Actor but the other parties would/could be actors
  - Does the Fee Exception apply?

Closing Discussion and Next Steps

- The group contemplated the potential impact of the COVID-19 to its work.
- Monthly calls are scheduled through May. If attention is diverted and work group participation is reduced, we can push the calls further out.

Discussion/Questions from April 2020 Meeting

Delayed Compliance and Infeasibility Exception

- We are in the midst of the COVID-19 crisis, with peak cases expected in the next few weeks and hope there will be declining cases in the summer. Assuming all goes well, it may be feasible to do the work needed to address information blocking-related work starting in the fall. Even if technically feasible at that point, it will not have been feasible to do the necessary preparation leading up to that point. There needs to be sufficient time to make changes in their systems and processes.
- Due to constraints/stress on providers due to the COVID-19 crisis, providers and other actors may have to rely on the Infeasibility Exception over the next 6-12 months unless compliance is delayed.
  - This exception is designed to address circumstances beyond the Actor's control, including public health emergencies. Look at the elements of the exception (e.g. substantial burden) and consider the facts and circumstances of a given sets of facts. The answer in every case seems to be that "it depends" on what the circumstances are.
  - Even if the requested means isn't feasible, the Actor has an obligation to identify alternative means to comply with the request. The burden is on providers and other Actors is to show you tried to comply and looked at alternative means to do so.
  - Do the Executive Order or emergency declaration produce presumptive infeasibility?
  - Question for ONC: can we use the infeasibility exception because it was infeasible when we intended to be building implementation and compliance plans, although "now" it would appear technically feasible?

Discussion/Questions from April 2020 Meeting

Delayed Compliance and Infeasibility Exception (continued)

- It will be important to link the Infeasibility Exception to broader compliance efforts and the activities that need to take place to prepare for the exceptions (e.g. licensing, fees, etc.).
  - Most exceptions, notably but not only Fee and Licensing, require compliance and implementation preparation, which would be tight with compliance and enforcement six months after publication of the Final Rule. If actors, especially providers, cannot use the 6-month period to address these, especially needed internal and external changes in fees and licensing and associated agreements because of the pandemic, that is a serious problem.
  - Can Actors use the infeasibility exception because it was infeasible to be building needed implementation and compliance plans to support data access, exchange and use and the ability to meet applicable exceptions, although meeting requests appears technically feasible?
  - Note: just because you fail to meet an exception doesn't mean you are violating the rule.
- Actors need clear direction from the Federal government regarding pandemic-related compliance and enforcement delays. Otherwise, thousands of individual actors will be forced to justify their collective delay with their own documentation and compliance planning.

Discussion/Questions from April 2020 Meeting

HIE/HIN

- Could providers, such as ACOs, be considered HINs?
  - Yes, based on the functions they provide
  - Suggestion: develop a checklist or decision map that helps providers determine if they are a HIN, especially as the information blocking definitions and penalties are different for these two categories of actors.

OIG Proposed Rule on CMPs

- Will this Work Group also focus on the forthcoming OIG Proposed Rule?
  - We will review the proposed rule and assess the extent to which it is focused primarily on technical legal issues. Overall, the provisions are likely broadly relevant and WG input and comments will likely be warranted.

Discussion/Questions from April 2020 Meeting

Content and Manner Exception

- It is important to understand how this exception interrelates with the Fee and Licensing exceptions.
- These latter exceptions only apply if the data holder cannot honor a request in "any manner requested".
- If can respond to the request in "any manner requested" and the requested manner happens to be one of the hierarchy of response options if "any manner" is not met, does the use of such an approach (e.g., ONC certification standard) mean that Fee and/or Licensing exceptions must be used?
  - Likely not
- If we are working through Content and Manner exception and move to alternative manners and still do not reach agreement, does the process end?
  - No. You could then turn to the Infeasibility exception, per ONC
  - But, there is a potential timing issue with that approach. The Infeasibility exception requires the Actor to respond to the request within 10-business days of the request outlining the reasons for claiming the request is infeasible and by the time an Actor completes stepping through the Content and Manner exception it could very likely already be past the 10-day requirement.

Discussion/Questions from April 2020 Meeting

Content and Manner Exception

- With information blocking compliance requirements starting 6-months after the final rule publication date and USCDI requirements for 2015 CEHRT Cures Updates being required two-years from the final rule publication date, there is an 18-month window of time in which information blocking requirements (specifically the Content and Manner exception that outlines the process to follow on receipt of a request) would enable a requestor to request functionality that is being developed and certified to meet certification requirements but has not been developed, tested, certified and/or GA.
  - *ONC Question: During this 18-month window, should requested functionality that aligns with the 2015 CEHRT Cures Update requirements be treated as complying with the manner requested under the Content and Manner exception or as complying with the alternative manner Certification/nationally adopted standards requirements? In addition, is it acceptable to inform the requestor that the requested functionality is under development and outline the expected timeline as part of the agreement under the Content and Manner exception?*

Discussion/Questions from April 2020 Meeting

Content and Manner Exception

- Under the Content and Manner Exception if a request is fulfilled in the manner requested, the actor need not comply with the Fees and Licensing exceptions but fulfilling a request in an alternative manner does require compliance with the Fee and Licensing exceptions.
  - The way this exception is worded could potentially allow for scenarios in which two requests are received, ultimately fulfilled in the same manner, but one would comply with the Fees and Licensing Exception and one would not. The example scenario would play out in years when the 2015 Edition Cures-related Updates are in effect and two requestors (requestor 1 and requestor 2) make similar requests to an Actor.
    - Requestor 1 makes a request for a standards-based API functionality using FHIR R4 for USCDI information and requestor 2 makes a request for a proprietary API to access USCDI. The Actor fulfills request 1 in the manner requested and does not need to comply with the Fees or Licensing exceptions. The Actor claims an inability to meet request 2 on technical reasons and moves to offer an alternative manner which is API access using FHIR R4, and the offer is accepted by the requestor. When the Actor completes request 2 it must meet the Fees and Licensing exceptions even though it is supplying the same functionality as in request 1.
  - *ONC question: Is this analysis correct and should this disparity be addressed or eliminated?*

- *ONC question: Does the Content and Manner exception allow for development time or an agreement to deliver a functionality after additional development? It is not clearly stated in the preamble or the regulation. There is mention of fulfilling the request without undue delay. Development time would add a delay, but would it be undue?*

Discussion/Questions from April 2020 Meeting

Fees and Licensing Exceptions

- *ONC question: If an actor works through the process of the Content and Manner exception and cannot reach an agreement on the manner requested or any of the alternative manners, does the actor have to claim Infeasibility or is lack of agreement enough? The rule seems to hint that the actor would claim Infeasibility however there is a potential timing issue with that. The infeasibility exception requires the actor to respond to the request within 10-business days of the request outlining the reasons for claiming the request is infeasible and by the time an actor completes stepping through the Content and Manner exception it could very likely already be past the 10-day requirement.*

Discussion/Questions from April 2020 Meeting

Fees and Licensing Exceptions

- *ONC question: ONC outlines that the 10-day and 30-day timelines required to meet the licensing exception are triggered by receipt of a request for license or use of EHI (p. 976) even when the requestor does not understand the need for a license. What needs to occur within the 30-day timeline? Do negotiations need to be completed within the 30-day timeframe?*
  - A 30-day timeline from the point of request to complete negotiations does not seem realistic for many scenarios.
- The Fees exception contains a condition that requires HIT Developers to comply with the Conditions of Certification related to EHI Export and APIs "for all practices and at all relevant times." The language seems to indicate that an HIT Developer would need to comply with Condition of Certification requirements for non-certified functionality.
  - *ONC question: Is the intent for Developers of certified health IT to comply with these conditions at all times for all certified modules, the wording is not clear and needs to be clarified.*
    - Staff: Some Conditions of Certification seem to be limited to certified health IT (e.g., for certified APIs) and others focus on the Actor's organization (e.g., information blocking).

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

21st Century Cures: Information Blocking (Section 4004)

A **practice** that:

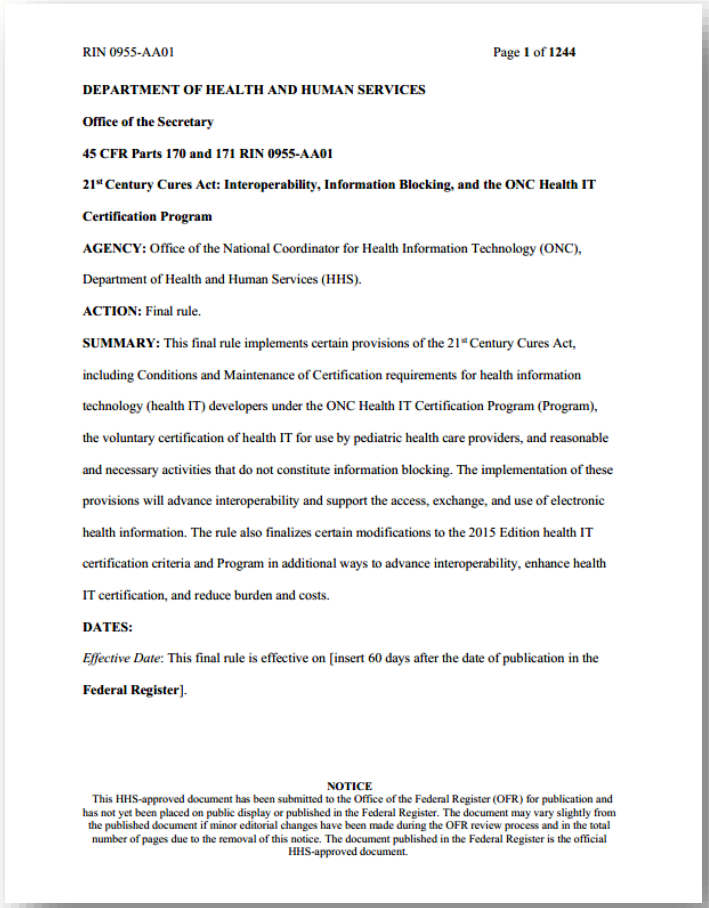
- Except as required by law or specified by the Secretary per ***rulemaking), likely*** to ***interfere with, prevent, or materially discourage access, exchange, or use*** of ***electronic health information*** (EHI); and
- If conducted by a **health IT *developer***, exchange, or network, developer,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

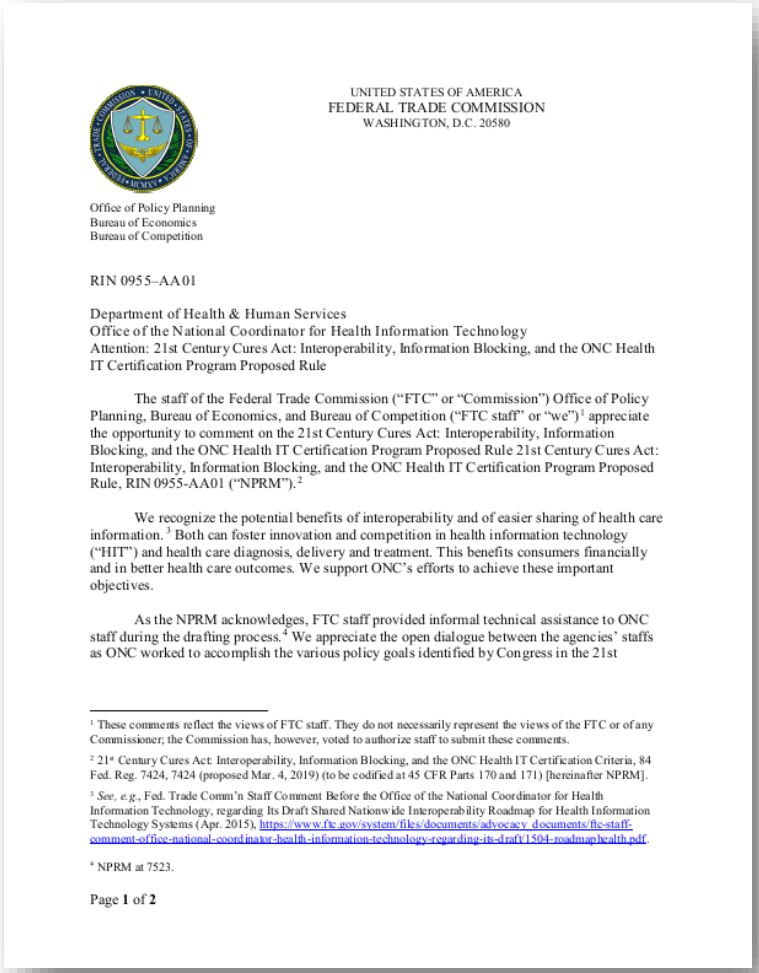
Final Rule—and not Interim Final Rule with Comments or Supplemental Notice of Proposed Rulemaking, as some requested:

> *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

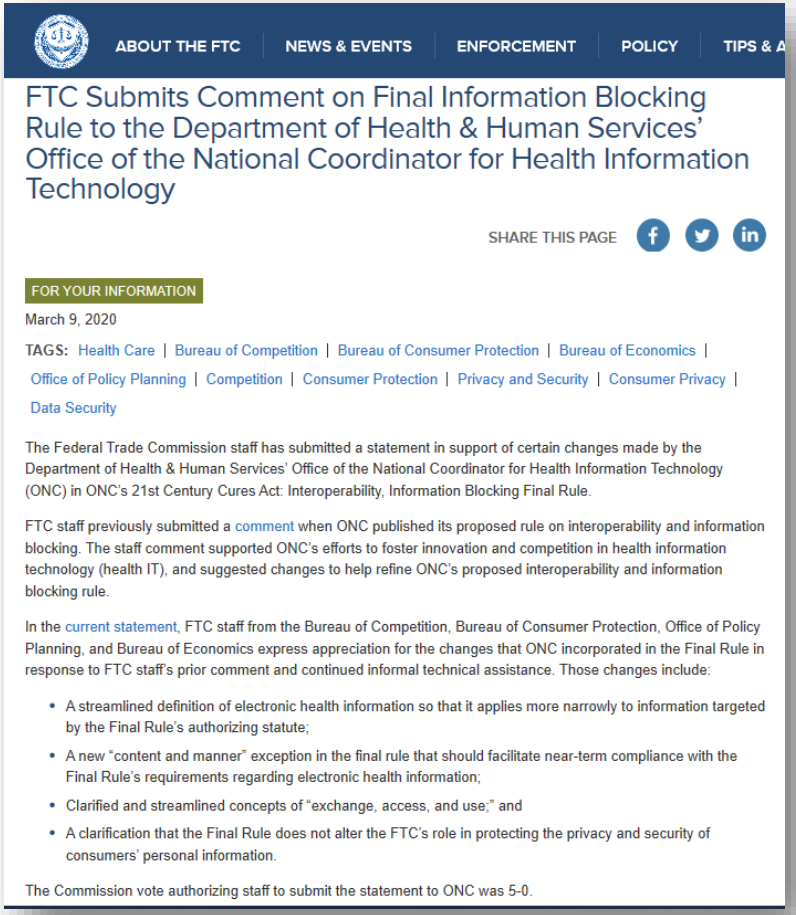
[1] These comments reflect the views of FTC staff. They do not necessarily represent the views of the FTC or of any Commissioner; the Commission has, however, voted to authorize staff to submit these comments.

[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 has finished OMB review)
- **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 "life or physical safety" retained where practice likely to, or does, interfere with patient's access, exchange, or use of their own EHI (per HIPAA 164.524(a)(3)(i). Otherwise, "substantial harm" standard
- 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; [substantial harm]

(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; [substantial harm]

(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 [life or physical safety]

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 published April 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

Appendix 2: 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)
  - Consider recent and future changes to 42 CFR Part 2 (e.g., from CARES Act)
  - 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
- ❑ Establish joint security governance across security/clinical information/operations teams to ensure consistent understanding and coordinated actions

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
- ❑ Prepare policies for documentation and other functions to support potential case-by-case assertions that a practice is not information blocking even if an exception does not apply
- ❑ 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