Information Blocking Bootcamp 2021
Information Blocking Summary

Introduction

This summary is a comprehensive resource to orient the reader to the Information Blocking provisions of the 21st Century Cures Act and the federal regulations that have been promulgated by the Office of the National Coordinator and the HHS Office of Inspector General. It presents an overview of the legal authority for the Information Blocking provisions and explains the many important components of this legal authority in logical framework. If you are new to the subject of Information Blocking, you will find this summary to be helpful as an overview; if you already familiar with Information Blocking, you will find helpful details about the provisions, including the exceptions, that will help your organization get prepared.

DISCLAIMER: This summary is NOT a substitute for legal advice. You should consult with legal counsel who is knowledgeable about the intricacies of the Information Blocking provisions and health information for questions that are specific to your organization.

This Information Blocking Summary© was prepared
by the digital health law firm

gravely GROUP

on behalf of The Sequoia Project, Inc.

Information Blocking Bootcamp 2021
Information Blocking Summary

SECTION 1: WHAT IS INFORMATION BLOCKING & HOW AND WHY IS IT PROHIBITED?

➢ IN THIS SECTION:

- We will start with a fundamental definition of what Information Blocking is and where the associated legal terminology and prohibition originated.
- We provide a brief background on:
  - The rationale on which Congress based its belief that Information Blocking is a problem in need of legislative and regulatory intervention; and
  - ONC's policy stance on Information Blocking.
- We begin to break down the Information Blocking definition into its discreet components, so that we can drill down more precisely into who and what is covered under the Information Blocking prohibition in the next sections.

➢ STAY TUNED FOR:

- Explanations
- Effects
- Examples
- Enforcement
- Exceptions

What is Information Blocking and What Prohibits It?

Statutory Basis

The 21st Century Cures Act (the "Cures Act")[1] prohibits "information blocking," and it is no accident that the Cures Act was enacted as part of the Public Health Services Act (PHSA). The PHSA is the comprehensive federal law that addresses the full spectrum of national public health matters, and Congress intentionally defined Information Blocking broadly to capture a wide spectrum of activities that it views as detrimental to the public health.

The Cures Act defines Information Blocking as "a practice that … is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information," ***unless*** **such practice is required by law** (e.g., HIPAA), **or it meets an exception established through federal rulemaking**.[2] The Cures Act also establishes two different intent requirements

[1] 21st Century Cures Act, Pub. L. No. 114-255 (2016).
[2] 42 U.S.C. § 300jj-52(a)(1).

for Information Blocking, based on the individual or entity engaging in an Information Blocking practice:

1. **A health information technology developer, exchange, or network must know or should know** that such practice is likely to interfere with access, exchange, or use of EHI;

2. **A healthcare provider must know** that such practice is unreasonable and likely to interfere with access, exchange, or use of EHI.

➢ **KEY DEFINITION**

Information Blocking is a **practice** that an **Actor knows or**, *in some cases*, **should know** is **likely to interfere** with **access**, **exchange**, or **use** of **electronic health information ("EHI")**.

Rules & Regulations

As the federal agency tasked with implementing Congress' Information Blocking prohibition, the Office of the National Coordinator for Health Information Technology ("ONC") published a proposed rule in March 2019, in which ONC put forth its interpretation and intended regulation of the Information Blocking prohibition for public comment (the "Proposed Rule").[3]

In May 2020, ONC published the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* final rule (the "Final Rule").[4] The Final Rule dispositions public comments ONC received in response to the Proposed Rule, provides insight into ONC's interpretation of the Cures Act Information Blocking prohibition, defines additional Information Blocking terms, **articulates Information Blocking exceptions**, and establishes the final text of the federal regulations governing Information Blocking.

PUT A PIN IN IT …

The Cures Act also includes a directive that the Secretary of HHS "identify reasonable and necessary activities that do not constitute information blocking" (i.e., exceptions) through federal rulemaking. In other words, given the breadth of the Information Blocking definition, Congress recognized the need to carve out certain practices that would otherwise constitute Information Blocking for specific protection as "reasonable and necessary" restraints on the access, exchange, or use of EHI.

MORE ON THE EXCEPTIONS TO COME!

[3] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health Certification Program, 84 Fed. Reg. 7424 (March 4, 2019, hereinafter the "Proposed Rule"), available at: https://www.federalregister.gov/d/2019-02224.

[4] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health Certification Program, 85 Fed. Reg. 25642 (May 1, 2020, hereinafter the "Final Rule"), available at: https://www.federalregister.gov/d/2020-07419.

Why Do Congress and ONC Consider Information Blocking Harmful?

Policy Background

Congress has been very concerned about allegations of Information Blocking in healthcare for many years. Congress ordered ONC to investigate Information Blocking and, in a 2015 report to Congress (the "2015 IB Report"),[5] ONC noted that Information Blocking results in several significant harms, including:

- It impedes progress towards reforming health care delivery and payment because sharing information seamlessly across the care continuum is fundamental to moving to a person-centered, high-performing health care system.
- It can undermine consumers' confidence in their health care providers by preventing individuals from accessing their health information and using it to make informed decisions about their health and health care.
- It not only interferes with effective health information exchange but also negatively impacts many important aspects of health and health care. To make informed health care decisions, providers and individuals must have timely access to information in a form that is usable.
- It prevents advances in biomedical and public health research, which require the ability to analyze information from many sources in order to identify public health risks, develop new treatments and cures, and enable precision medicine.[6]

Since the 2015 IB Report, ONC has continued to assess the extent and nature of Information Blocking in healthcare. In its Proposed Rule, ONC stated that "based on these economic realities and our first-hand experience working with the health IT industry and stakeholders, in the Information Blocking Congressional Report, we concluded that information blocking is a serious problem and recommended that Congress prohibit information blocking and provide penalties and enforcement mechanisms to deter these harmful practices."[7]

[5] U.S. Dept. of Health and Human Services, Office of the National Coordinator for Health Information Technology: Report on Health Information Blocking (April 2015, hereinafter the "2015 IB Report").
[6] 2015 IB Report at 8.
[7] Proposed Rule at 7508.

What Are the Key Components of the Information Blocking Definition & What Do They Mean?

First, let's take another look at **the fundamental definition of Information Blocking:**

> **Information Blocking** is a **practice** that an **Actor knows or**, *in some cases*, **should know** is **likely to interfere** with **access**, **exchange**, or **use** of **electronic health information ("EHI")**.

Now, let's break down **the different components of the definition and what they mean:**

- "**practice**" – This is defined as "an act or omission" by an Actor.[8] The definition of "practice" focuses on what an Actor does or fails to do versus what it meant to do. Under this definition, the actual conduct of the Actor will be examined to decide whether the Actor engaged in Information Blocking (whether through affirmative action or through inaction). This term is extremely broad and can include business practices, technology, and/or how the Actor is structured.
- "**likely to interfere**" – The term "**interfere**" is defined in the Final Rule to mean "**prevent**, **materially discourage**, or otherwise **inhibit**."[9] However, the most important word to focus on here is "**likely**."
    - ***Actual interference is not required to meet the definition of Information Blocking.***
    - Practices that have a mere ***likelihood*** of interfering with the access, use, or disclosure of EHI are considered to be Information Blocking and are prohibited.
    - The government does not need to show that an Actor *actually* prevented, discouraged, or inhibited access, exchange, or use of EHI.
    - **It is enough to violate the Information Blocking statute if an Actor's practices are *likely to interfere with (i.e., prevent, materially discourage, or otherwise inhibit)* access, exchange, or use of EHI.**
- "**access, exchange, or use**" – Some think that the Information Blocking Rule only applies to the sharing of electronic health information between networks. This assumption is incorrect and could expose organizations to significant liability. Information Blocking certainly applies to the exchange of EHI, but it also extends to the access and use of EHI both within and across healthcare organizations.

---

[8] Final Rule at 25955.

[9] Final Rule at 25956. Note that, in addition to defining interference in the Final Rule, ONC initially defined Information Blocking to include a practice that is likely to "interfere with, prevent, or materially discourage access, exchange, or use of EHI." (Final Rule at 25956.) In a corrections and clarifications section in a subsequently published Interim Final Rule, ONC clarifies, "The definition of information blocking … should not include 'prevent, or materially discourage.' It is redundant and could confuse stakeholders… ." *See*, Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency, 85 Fed. Reg. 70064 at 70078 (Nov. 4, 2020, hereinafter the "Interim Final Rule"), available at: https://www.federalregister.gov/d/2020-24376.

- "**Access**" means "the ability or means necessary to make electronic health information available for exchange or use."[10]
- "**Exchange**" means "the ability for electronic health information to be transmitted between and among different technologies, systems, platforms or networks."[11]
- "**Use**" means "the ability for electronic health information, once accessed or exchanged, to be understood and acted upon."[12]

The breadth of these terms is important to understand for an organization to accurately assess its risk for **Information Blocking penalties**.

> **PUT A PIN IN IT …**
>
> The **Office of Inspector General (OIG)** is responsible for certain enforcement aspects of Information Blocking, including the imposition of civil monetary penalties (CMPs).
>
> **Enforcement will be addressed toward the end of this summary.**

- "**actor**" – An Actor is a (1) **healthcare provider**, (2) **health IT developer of certified health IT**, and/or (3) **health information exchange / health information network**. We will further unpack the definition of each of these types of Actors in the next section of this summary.
- "**knows or should know**" – Intent is an essential element of whether an Actor has engaged in Information Blocking. ONC has made clear that it does not intend to punish anyone for "innocent mistakes." There must be *some* element of intentionality in order for a practice to meet the definition of Information Blocking. It is important to note that **the intent needed to prove Information Blocking is not the same for all Actors:**
  - **Healthcare providers** are liable for a practice that the healthcare provider ***knows is unreasonable and is likely to interfere*** *with* access, use, or exchange of EHI. This means that a healthcare provider must have **actual knowledge**, which is a higher standard of proof than it is for all other Actors. Healthcare providers must also know that the practice is **unreasonable**.
  - **All other Actors** are liable for a practice that the Actor **knows *or should know* is likely to interfere** with access, use, or disclosure of EHI. Actual knowledge is NOT required for such a practice to be considered Information Blocking. These Actors cannot simply turn a blind eye and claim that they did not realize that their practices would prevent, materially discourage, or otherwise interfere with the access, exchange, or use of EHI; such Actors are liable if they ***should have known*** that their practice would likely interfere with access, exchange, or use of EHI.
- "**electronic health information (EHI)**" – Generally speaking, the definition of EHI tracks the definition of ePHI under HIPAA. However, there are some nuances that we discuss later in this summary.

[10] Final Rule at 25955.
[11] Final Rule at 25955.
[12] Final Rule at 25956

SECTION 2: WHO IS REGULATED UNDER THE INFORMATION BLOCKING RESTRICTIONS

As stated in Section 1, the Information Blocking prohibition applies to **Actors**.

➢ KEY DEFINITION

For purposes of the Information Blocking restrictions, **Actors** are (1) **Healthcare Providers**, (2) **Health IT Developers of Certified Health IT**, and/or (3) **Health Information Networks (HINs)** and **Health Information Exchanges (HIEs)**.

Who/What Are "Healthcare Providers" Under ONC's Final Rule?

For purposes of Information Blocking, ONC utilizes the same definition of **"health care provider"** as under the Public Health Services Act.[13] This definition is extremely broad and includes the following **individuals and entities:**

- hospitals
- skilled nursing facilities, nursing facilities, and/or other long-term care facilities
- home health entities
- health care clinics
- community mental health centers
- renal dialysis facilities
- blood centers
- ambulatory surgical centers
- emergency medical services providers
- federally qualified health centers
- group practices
- pharmacists / pharmacies
- laboratories
- physicians
- practitioners (physician assistants, nurse practitioners, clinical nurse specialists, certified registered nurse anesthetists, certified nurse-midwives, clinical social workers, clinical psychologists, and registered dietitians or nutrition professionals)
- providers operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization
- rural health clinics

[13] Final Rule at 25955, citing 42 U.S.C. § 300jj(3).

- covered entities under 42 U.S.C. § 256b[14]
- ambulatory surgical centers
- therapists
- any other category of healthcare facility, entity, practitioner, or clinician determined appropriate by the Secretary

So, a healthcare provider for purposes of the Information Blocking Rule is essentially any/every individual or entity that provides healthcare services. The burden would be upon an individual or entity to prove that he/she/it is NOT an Actor. ONC made clear in its first set of Frequently Asked Questions (FAQs), published in 2020, that this definition does not require the use of health IT that is certified under the ONC Health IT Certification Program.[15]

Who/What Are "Health IT Developers of Certified Health IT" Under ONC's Final Rule?

➢ **KEY TAKEAWAY**

A **health IT developer of certified health IT** is (1) an **individual or entity** (2) that **develops or offers Health Information Technology** (3) ***AND*** has **one or more Health IT Modules certified** under ONC's Health IT Certification Program (4) **at the time such individual or entity engages in a "practice"** that is the subject of an Information Blocking claim.

ONC excludes from the definition of a health IT developer of certified health IT "a health care provider that self-develops health IT for its own use."[16] However, organizations or individuals that act as "resellers" of certified Health IT *are* covered by this definition and *are* Actors.[17]

Interestingly, the definition of a health IT developer of certified health IT (hereinafter referred to as a "Certified HIT Developer") expressly includes engaging in the practice of Information Blocking. Neither the definition of healthcare provider nor HIN/HIE have this distinction. The other types of Actors simply are Actors, *regardless* of whether they engage in practices that could be Information Blocking.

ONC recognized that its authority over the actions of health IT developers only extends to those developers that have ONC-certified health IT. Therefore, ONC clearly intended to limit its reach under Information Blocking to Certified HIT Developers, a status that may change over time. This is why it was important for ONC to specify that a health IT developer is only an Actor while

[14] Note that this is NOT the definition of a "covered entity" under HIPAA. The definition of covered entity for purposes of the ONC Info Blocking Rule is at 42 U.S.C. § 256b(a)(4).
[15] ONC, *Information Blocking FAQs*, (Nov. 2020), available at https://www.healthit.gov/curesrule/resources/information-blocking-faqs, accessed Jan. 13, 2021, (hereinafter, the "ONC FAQs (2020)").
[16] Final Rule at 25956.
[17] ONC FAQs (2020), available at https://www.healthit.gov/curesrule/resources/information-blocking-faqs.

the health IT developer has one or more ONC-certified Health IT Modules. However, what the final regulatory text says is that a Certified HIT Developer is "an individual or entity … that develops or offers health information technology … and which has, at the time it *engages in* ***a practice that is the subject of an information blocking claim,*** one or more [ONC-certified] Health IT Modules… ."[18]

While it was clearly ONC's intent to limit the definition of health IT developers to only those that offer certified health information technology at the time of the Information Blocking practice, the Final Rule adds another requirement to the definition: A Certified HIT Developer must also **"engage[] in a practice that is the subject of an information blocking claim."** ONC states in the Final Rule that, because the Public Health Services Act, including as amended by the Cures Act, does not define a "health IT developer," ONC decided to link this definition to the authority of OIG to enforce the Information Blocking provisions. ONC determined that this was the most effective approach.[19]

This creates a bit of complexity. Does a Certified HIT Developer only become an Actor when it engages in a practice that is the subject of an information blocking claim? That is **not** conventional wisdom regarding ONC's intent. However, we cannot ignore the fact that the *regulatory text* includes this language and, *in the narrative*, ONC tells us why the text is written this way. This may well be a matter that is litigated down the road if a health IT developer contests that it is subject to ONC's jurisdiction under the Information Blocking Rule because it was not "engage[d] in a practice that was the subject of an information blocking claim." A discussion of how a court might rule on this question is beyond the scope of this Bootcamp, but it is interesting to consider. Notably, however, it is the certified health IT Module and the Information Blocking practice that is claimed that must be contemporaneous. The actual claim that a developer engaged in an Information Blocking practice could come after-the-fact. **An obvious takeaway is that every Certified HIT Developer should assume that it is an Actor and is subject to enforcement by the OIG.**

Who/What Are "Health Information Networks" & "Health Information Exchanges" Under ONC's Final Rule?

➢ **KEY TAKEAWAY**

ONC applies a functional definition of a **health information network (HIN) or health information exchange (HIE)** (provided below) that focuses on what an **individual or entity** actually **does**, **or has the authority to do**, rather than on how it is organized, what it is called, or what type of legal entity it is.

The definition is extremely broad, and there are likely organizations that do not consider themselves HINs/HIEs that will fall within this functional definition.

[18] Final Rule at 25956 (emphasis added).
[19] Final Rule at 25795.

A "**Health information network** or **health information exchange**" is:

> [A]n **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**.[20]

Let's further unpack this definition:

- 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** – ONC clearly contemplates that Actors may be individuals, as well as entities. Here, we see that particular individuals with the authority to direct how technology or services are used for the access, exchange, or use of EHI would be Actors under this definition and, therefore, can be individually culpable for something like an organizational policy that constitutes Information Blocking.
- Among **more than two unaffiliated** individuals or entities (**other than the individual or entity to which this definition might apply**) – ONC states in the Final Rule that this qualification is intended to "ensure[ ] that the definition does not unintentionally cover what are essentially bilateral exchanges in which the intermediary is simply performing a service on behalf of one entity in providing EHI to another or multiple entities and no actual exchange is taking place among all entities… ."[21]
- That are **enabled to exchange** with each other – "[T]o be enabled, the parties must have the ability and discretion to exchange with each other under the policies, agreements, technology, and/or services."[22]
- **That is for a treatment, payment, or health care operations purpose**, … **regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164** – The important thing to note about this part of the definition is that, although the exchange of EHI in this context must be for treatment, payment, or

[20] Final Rule at 25955-56 (emphasis added).
[21] Final Rule at 25802.
[22] Final Rule at 25802.

healthcare operations as defined under HIPAA, the individual or entity need not be subject to HIPAA to be an Actor under this definition. It is also worth noting that the exchange of EHI for treatment, payment, or healthcare operations is merely a threshold requirement to meet the definition of an HIN/HIE for purposes of being an Actor; if an individual or entity meets this definition of an HIN/HIE, then the Information Blocking prohibitions apply to the access, exchange, or use of EHI for any purpose.

ONC made clear in its first set of Frequently Asked Questions (FAQs), published in 2020, that this definition does *not* require the use of health IT that is certified under the ONC Health IT Certification Program.[23]

Did We Forget Someone?

Notably absent from the definition of Actors are health plans. This means that **a health plan is not subject to the Information Blocking Rule while operating as a health plan**. *However*, if a health plan developed certified health IT or operated a HIN/HIE, the health plan would become subject to the Information Blocking Rule for those activities.

[23] ONC FAQs (2020), available at https://www.healthit.gov/curesrule/resources/information-blocking-faqs.

SECTION 3: WHAT TYPE OF ACTIVITIES WILL BE CONSIDERED INFORMATION BLOCKING?

The Cures Act includes business, technical, and organizational practices as potentially resulting in Information Blocking, and the statute includes several categories of Information Blocking practices, quoted in their entirety below.

> (A) practices that restrict authorized access, exchange, or use under applicable State or Federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health information technologies;
>
> (B) implementing health information technology in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information; and
>
> (C) implementing health information technology in ways that are likely to—
>
> (i) restrict the access, exchange, or use of electronic health information with respect to exporting complete information sets or in transitioning between health information technology systems; or
>
> (ii) lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health information technology.[24]

In addition, in the Proposed Rule, **ONC listed 42 examples of specific activities** ☆ that *could* constitute a practice resulting in Information Blocking. Using this framework, these 42 specific practices can be organized into the following categories:

See **Appendix 1 for ONC's list of Specific Practices**

- Restricting access, exchange, or use
- Limiting or restricting health IT interoperability
- Impeding innovations and advancement in access, exchange, or use or in health IT-enabled care delivery
- Engaging in rent-seeking and other opportunistic practices
- Engaging in non-standard implementation practices

This list of examples is extremely extensive and covers many activities that happen every day in the healthcare system. ONC acknowledges this in the Final Rule but goes to great lengths to emphasize that even this very extensive list is not exhaustive. ONC states, "we stressed that

[24] 42 U.S.C. § 300jj-52(a)(2).

the types of practices discussed in the preamble of the Proposed Rule are illustrative and ***not exhaustive*** and that ***many other types of practices could also implicate the provision.***"[25]

ONC included the list of practices in the Proposed Rule to illustrate the scope of the Information Blocking provisions. ONC states in the Final Rule that it wanted to make clear that "because information blocking can take many forms, it is not possible to anticipate or catalog all potential types of practices that may raise information blocking concerns."[26] **Therefore, even practices that are not listed in the Proposed Rule cannot be considered "safe."** ONC specifically states in the Final Rule that "the fact that we did not identify or discuss a particular type of practice did not imply that it is less serious than those that were discussed in the Preamble."[27]

In addition, the term "practice" can create a little bit of confusion, since one may be tempted to think of a practice as actively doing something. It is important to remember that a "practice" is defined in the Final Rule as "an act ***or omission*** by an actor."[28] **An Actor can engage in Information Blocking not only by affirmatively *doing* something but also by *failing to do something* that is required.**

So, what does this mean?

➢ **KEY TAKEAWAY**

It means that all Actors must be extremely careful in evaluating their risk profile for Information Blocking and carefully consider every aspect of how they deal with EHI, especially with respect to requests for access, exchange, or use of EHI. Actors must think about their risk of Information Blocking very expansively and think about both the actions they take *AND* the actions that they fail to take.

[25] Final Rule at 25808 (emphasis added).
[26] Final Rule at 25808.
[27] Final Rule at 25808.
[28] Final Rule at 25955 (emphasis added).

SECTION 4: IS *EVERY* PRACTICE AN INFORMATION BLOCKING VIOLATION?

The good news is "no," not every "practice" means that an Actor has violated the Information Blocking prohibition.

REMEMBER:

There are additional elements required to constitute Information Blocking, including:

- The practice must be **likely to interfere** with the access, use, or exchange of EHI;
- A healthcare provider must **know** that the practice is unreasonable and that the practice is likely to interfere with the access, use, or exchange of EHI;
- All other Actors must know, **or should know**, that the practice is likely to interfere with the access, use, or exchange of EHI; and
- The practice must involve the access, use, or exchange of **EHI**.

Interference

As noted in Section 1, "interference" means "to prevent, materially discourage, **or otherwise inhibit**" the access, exchange, or use of EHI.[29] ONC states that interference may take many forms other than actually preventing or materially discouraging access, use, or exchange of EHI and can include practices that:

- "increase the cost, complexity, or other burdens associated with accessing, exchanging, or using EHI"; or
- "limit the utility, efficacy, or value of EHI … by diminishing the integrity, quality, completeness, or timeliness of the data."[30]

Likelihood of interference

An Actor's practice does not have to *actually* interfere with access, use, or exchange of EHI to be an Information Blocking violation. The fact that practices that are ***likely*** to interfere, but do not actually interfere, constitute Information Blocking dramatically expands the scope of the Information Blocking Rule. ONC states that by including both the likely and the actual effects of a practice, individuals and entities are encouraged to "avoid engaging in practices that

[29] Final Rule at 25956 (emphasis added).
[30] Final Rule at 25809.

undermine interoperability, and to proactively promote access, exchange, and use of EHI."[31] So, Actors need to both "avoid" and "promote" as part of their Information Blocking compliance.

➢ **KEY TAKEAWAY**

ONC states that **a practice is likely to interfere "if, under the circumstances, there is a reasonably foreseeable risk that the practice will interfere with access, exchange, or use of EHI."**

ONC states that the particular facts and circumstances of the practice will determine whether the risk of interference is reasonably foreseeable.[32] This does not provide the clarity that many commenters sought, but **the list of 42 examples of specific practices in the Proposed Rule** are ONC's guidance on specific practices that are likely to interfere with access, exchange, or use of EHI and, therefore, be a violation unless there is an applicable exception.[33]

Knowledge

As already discussed, healthcare providers must have actual knowledge that a practice is both unreasonable and is likely to interfere with access, exchange, or use of EHI. All other Actors, can be liable for practices that they either knew, or should have known, were likely to interfere with access, exchange, or use of EHI.

The terms "know" and "should know" are not defined in the Cures Act or in the Information Blocking Rules (Proposed or Final), which means that a common usage of these terms will likely be employed for investigations and enforcement.

Electronic Health Information (EHI)

The Final Rule defines EHI as follows:

> "Electronic health information (EHI)" means 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 160.501, 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

[31] Final Rule at 25809.
[32] This and the preceding quote are at 25809 in the Final Rule.
[33] Final Rule at 25809.

(2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[34]

Under the Final Rule, EHI is also ***initially*** limited to the electronic health information identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard (but not the associated standards). This limitation lasts until October 6, 2022, unless it is extended by ONC, again, in subsequent rulemaking.[35]

The definition of EHI was modified from the definition included in the Proposed Rule in response to numerous comments that expressed concerns about the confusion that the proposed definition of EHI would create for HIPAA covered entities and their business associates, since the proposed definition of EHI was broader than the HIPAA definition of ePHI. ONC narrowed the definition of EHI to have it track the HIPAA definition of ePHI to avoid the burden on HIPAA covered entities and their business associates of needing to differentiate and track both ePHI under HIPAA and EHI under the Information Blocking regulations.[36]

[34] Final Rule at 25955.
[35] The original end-date for the limitation provided in the Final Rule was May 2, 2020 (at 25793). This timeframe was adjusted, along with the overall applicability date, in the Interim Final Rule (at 70085).
[36] Final Rule at 25803-04.

SECTION 5: WHAT HAPPENS IF AN ACTOR ENGAGES IN INFORMATION BLOCKING?

Enforcement and Penalties

The Cures Act authorizes the U.S. Department of Health and Human Services (HHS) Office of Inspector General (OIG) to investigate claims of Information Blocking and provides the Secretary of HHS the authority to impose civil money penalties (CMPs) for Information Blocking.

- **Actors that are healthcare providers are not subject to these CMPs.**
- **All other Actors are subject to CMPs of up to $1,000,000 per occurrence.**

The OIG published a Proposed Rule on April 24, 2020, to explain how OIG will investigate allegations of Information Blocking, provide insight into how it will determine whether a CMP should be imposed, and seek public comment on how it should determine the amount of any CMP (the "OIG Proposed Rule").[37]

OIG notes that many of the individuals and entities that are subject to Information Blocking may not be familiar with OIG's enforcement authorities. Therefore, OIG includes information in the OIG Proposed Rule about its enforcement authority and its anticipated approach to Information Blocking. OIG states that it plans to draw on its longstanding experience investigating healthcare fraud when dealing with allegations of Information Blocking, and OIG notes that it will follow similar methods and techniques that are "tailored to each complaint's unique facts and circumstances."[38]

OIG has the discretion to decide which allegations to investigate. In making that determination, OIG states that it will consider the following:

1. Did the conduct result in, cause, or have the potential to cause **patient harm**?
2. Did the conduct significantly impact a healthcare **provider's ability to care for patients**?
3. Was the conduct of **long duration**?
4. Did the conduct **cause financial loss** to any federal healthcare program or other government or private entities?
5. Was the conduct performed with **actual knowledge**?[39]

OIG states that these factors will likely evolve as OIG gains more experience investigating Information Blocking.[40]

---

[37] Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules, 85 Fed. Reg. 22979 (April 24, 2020, hereinafter the "OIG Proposed Rule"), available at: https://www.federalregister.gov/d/2020-08451.

[38] OIG Proposed Rule at 22984.

[39] OIG Proposed Rule at 22984.

[40] OIG Proposed Rule at 22984.

OIG affirms that it has no authority to pursue Information Blocking CMPs against Actors that did not act (or fail to act) with the **requisite intent**.

REMEMBER:

(1) Healthcare Providers are not subject to these CMPs; and

(2) The "requisite intent" for all other Actors (i.e., Certified HIT Developers and HINs/HIEs) is that they *knew or should have known* that the practice in question was likely to interfere with the access, use, or exchange of EHI.

In the OIG Proposed Rule, the agency states "OIG will not bring enforcement actions against Actors who OIG determines made innocent mistakes."[41]

For healthcare providers, if OIG determines the provider engaged in Information Blocking, OIG will refer the provider to "the appropriate agency to be subject to appropriate disincentives," which will be established in future rulemaking.[42]

For all other Actors, OIG will determine the amount of CMPs to assess based, in part, on the number of "violations" the Actor has committed. OIG is proposing to tie the number of violations to the number of practices that the Actor committed. The OIG Proposed Rule provides examples of situations in which an Actor would be considered to have committed a single violation or multiple violations.[43]

The Cures Act mandates that the determination to impose CMPs for Information Blocking must include consideration of certain factors, including, as applicable:

- **The nature and extent of the Information Blocking**
- **The resulting harm**
- **The number of patients affected**
- **The number of provides affected**
- **The number of days the Information Blocking persisted.**[44]

OIG also sought comment on any additional factors that it should consider in determining the amount of CMPs to assess against an Actor.[45]

[41] OIG Proposed Rule at 22984.
[42] Final Rule at 25900.
[43] OIG Proposed Rule at 22986-87.
[44] OIG Proposed Rule at 22987.
[45] OIG Proposed Rule at 22987.

SECTION 6: WHEN IS A PRACTICE THAT MAY CONSTITUTE INFORMATION BLOCKING NONETHELESS PERMISSIBLE?

What is an Exception?

The Cures Act includes a directive that the Secretary of HHS "identify reasonable and necessary activities that do not constitute information blocking" through federal rulemaking.[46] In other words, given the breadth of the Information Blocking definition, Congress recognized the need to carve out certain practices that would otherwise constitute Information Blocking for specific protection as "reasonable and necessary" restraints on the access, exchange, or use of EHI. Pursuant to that directive, ONC developed certain "exceptions" for practices that, while meeting the definition of Information Blocking, will not be punishable as such.

ONC identified **three overarching policy considerations** undergirding each exception:

1. The exceptions are limited to certain activities that ONC believes are "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. The exceptions are intended to address what ONC considers a "significant risk" that Actors would otherwise avoid engaging in activities that are reasonable and necessary out of concern that such activities could be interpreted as Information Blocking.

3. The exceptions are intended to be "tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt."[47]

The exceptions consist of practices that are "reasonable and necessary" for an Actor to engage in *even though the practices meet the definition of Information Blocking*.

The exceptions provide an affirmative defense to an allegation that an Actor engaged in Information Blocking. This means that even if an Actor engaged in a practice that it knew, or should have known, was likely to interfere with the access, exchange, or use of EHI, the Actor will not be held liable for Information Blocking if the practice falls within an exception. This is an extraordinary remedy that is available to Actors. Therefore, ONC crafted each exception with the intent that it be narrowly tailored and limited to the specific activities that ONC intends it to exempt.

[46] 42 U.S.C. § 300jj-52(a)(3).
[47] Final Rule at 25649.

The Final Rule identifies ***eight* exceptions**, which is one more than ONC proposed in the Proposed Rule. ONC also made some important revisions to the exceptions in the Final Rule.

- **Exceptions 1-5 involve not fulfilling requests to access, exchange, or use EHI.**
- **Exceptions 6-8 involve procedures for fulfilling requests to access, exchange, or use EHI.**[48]

See **Appendix 2 for ONC's comparison of key provisions in the Final Rule vs. the Proposed Rule, including changes to the exceptions.**

ONC also points out, in the Final Rule, that it uses the term "fulfill" throughout the exceptions. The context is almost always in terms of an Actor "fulfilling" a request to access, exchange, or use EHI. ONC states that its **use of the term "fulfill" is intended to reinforce that Actors will not just respond to requests to access, exchange, or use EHI but that they will actually make the EHI available** for the requested access, exchange, or use.[49] The impact of this cannot be overstated.

The Role of Exceptions in an Information Blocking Investigation

The Information Blocking exceptions provide protection for practices that would otherwise be Information Blocking. If an Actor is being investigated by OIG for an alleged Information Blocking violation (see Section 5), the Actor can assert that the alleged Information Blocking practice fell within an exception. The burden is squarely on the Actor to demonstrate that an exception is applicable and that the Actor met all relevant conditions of the exception at all relevant times and for each practice for which the exception is sought.[50]

➢ **KEY TAKEAWAY**

To meet an exception, the Actor must demonstrate that it met *ALL* of the requirements of the applicable exception. Meeting *most* of the requirements of an exception (or a combination of partial requirements from different exceptions) is NOT sufficient to fit within the safe harbor of an exception.

However, ONC makes clear in the Final Rule that an Actor's failure to meet an exception does not *automatically* mean that the Actor engaged in Information Blocking.[51] Just because there is no relevant exception, or the Actor fails to meet all of the requirements of an applicable exception, does not mean that the Actor will *necessarily* be found to have engaged in Information Blocking. The OIG must still determine that the practice that is the focus of the

[48] Final Rule at 25649.
[49] Final Rule at 25821.
[50] Final Rule at 25819.
[51] Final Rule at 25820.

allegation meets the definition of Information Blocking. As noted previously, this includes determining that:

(1) The practice was **likely to interfere** with **access, exchange, or use of EHI**; *and*

(2) The Actor had the **requisite intent** when it engaged in the practice (i.e., actual knowledge for health care providers and "knew or should have known" for all other Actors)

What are the Exceptions?

EXCEPTIONS THAT INVOLVE NOT FULFILLING REQUESTS TO ACCESS, EXCHANGE, OR USE ELECTRONIC HEALTH INFORMATION

1. **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?**[52]

➢ **KEY TAKEAWAY**[53]

The Preventing Harm Exception is intended to "allow for the protection of patients and other particular persons against substantial risk of harm" that may arise from access, exchange, or use of EHI in defined circumstances.

ONC voiced concern that, if not narrowly tailored, the exception could be used either as a pretext or a post-hoc rationalization for not sharing EHI; therefore, ONC imposes strict conditions on the use of this exception.[54] **In order to meet the exception, the Actor must:**

(1) Have a **reasonable belief** that the practice will **substantially reduce** the **risk of the harm** to a patient or another natural person;

(2) Ensure the practice is **no broader than necessary** to substantially reduce the risk of harm; and

(3) Meet at least one of the specified conditions from each of the established categories: **type of risk**, **type of harm**, and **documented basis of determination**.[55]

[52] Final Rule at 25956-57.
[53] Final Rule at 25821.
[54] Final Rule at 25822.
[55] Final Rule at 25956-57.

The **Type of Risk** must either:

(1) "Arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason."[56]

- ONC stresses that this exception will not apply if there is "mere speculation" that EHI is misidentified or mismatched, corrupt, or erroneous. ONC notes that the exception must be based on facts.
- In its Proposed Rule ONC specifically referred to 42 C.F.R. Part 2 data as an example, stating that the Part 2 regulations are not a broad shield to prevent disclosing anything in the patient's record.[57] This point is extremely important since providers have often withheld the entire record because they cannot parse out Part 2 information.[58]
- ONC also noted in the Proposed Rule that incompleteness of a patient record is not considered an inaccuracy.[59]

OR

(2) "Be determined on an individualized basis in the exercise professional judgement 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."[60]

- The existence of a current or previous clinician-patient relationship is essential because the risk of harm is specific to the individual patient.[61]
- The healthcare professional has broad discretion to consider all aspects of the individual patient when making their determination.[62]

The **Type of Harm** must be one that could serve as grounds for a HIPAA covered entity to deny access to an individual's Protected Health Information. ONC deliberately aligned this exception with HIPAA to promote consistency and minimize confusion.[63]

---

[56] Final Rule at 25956.
[57] Proposed Rule at 7524.
[58] ONC did, however, clarify in the Final Rule that, if an Actor truly lacks the technical capability to effectively segment such data, the Actor should consider the Infeasibility Exception (which specifically addresses the inability to segment data) or the new Content and Manner Exception. Final Rule at 25825-26.
[59] Proposed Rule at 7524.
[60] Final Rule at 25956.
[61] Final Rule at 25836.
[62] Final Rule at 25836-37.
[63] Final Rule at 25956.

The Final Rule identifies **four specific circumstances and the type of harm to which each circumstance must give rise**:

(1) Interfering with access, exchange, or use of EHI by the patient's legal representative based on an individualized determination of risk of harm by a licensed healthcare professional in the exercise of professional judgement. The specific type of harm that the Actor believes its practice will substantially reduce is **"substantial harm to the individual or another person."**

(2) Interfering with the patient's or their legal representative's access, exchange, or use of EHI that references another natural person based on an individualized determination of risk of harm by a licensed healthcare professional in the exercise of professional judgement. The specific type of harm that the Actor believes its practice will substantially reduce is **"substantial harm to such other person."**

(3) Interfering with the patient's access, exchange, or use of their own EHI based on an individualized determination of risk of harm by a licensed healthcare professional in the exercise of professional judgement OR based on data that are known or reasonably suspected to be corrupt due to technical failure, are erroneous for another reason, or are misidentified or mismatched. The specific type of harm that the Actor believes its practice will substantially reduce is **"harm to the life or physical safety of the individual or another person."**

(4) Interfering with a legally permissible access, exchange, or use of EHI that is not otherwise described in (1)-(3) above and regardless whether the **Type of Risk** is consistent with (1) or (2) on the preceding page. The specific type of harm that the Actor believes its practice will substantially reduce is **"harm to the life or physical safety of the individual or another person."**[64]

> ➢ **NOTE: "harm to the life or physical safety of the individual or another person"** is a very high standard that many current practices will likely fail to meet.

The **Documented Basis of Determination**:

ONC specifies two ways that the Preventing Harm Exception may be implemented:

(1) An **organizational policy**; and/or

(2) A **determination of risk of harm**.[65]

The Final Rule includes a specific process for developing an organizational policy for purposes of meeting the exception. **The organizational policy must be:**

[64] Final Rule at 25957.
[65] Final Rule at 25957.

a. A written policy;
b. Developed with meaningful input from clinical, technical, and other staff with specific expertise;
c. Implemented in a consistent and non-discriminatory manner; and
d. No broader than necessary to address the harm being prevented. The policy needs to identify the harm being targeted and how the policy mitigates that harm. There must also be evidence that the Actor considered alternative approaches and determined that they would not be effective.[66]

ONC recognizes that an organizational policy cannot address every situation and that small medical practices, in particular, might not be able to adopt such policies. So, the rule also allows an Actor to make an individualized determination of risk of harm based on the facts and circumstances present in a specific situation that disclosing EHI might cause harm to the patient or another person. **The requirements for such a determination are:**

a. The facts and circumstances must be known or reasonably believed by the Actor at the time the determination was made and while the practice remains in use; and
b. The determination must be based on expertise relevant to implementing the practice consistent with the requirements of this exception.[67]

[66] Final Rule at 25957.
[67] Final Rule at 25957.

2. 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?[68]

➢ **KEY TAKEAWAY**

The Privacy Exception is intended to "allow for the protection of patients and other particular persons against substantial risk of harm" that may arise from access, exchange, or use of EHI in defined circumstances.

This exception is unique in that it has 4 discrete sub-exceptions, and **an Actor must meet all of the requirements under at least one of these sub-exceptions to use this exception.**[69]

a. ***Sub-exception 1: Precondition not satisfied.*** The first sub-exception applies if applicable law imposes a specific precondition that must be satisfied before information can be released, and that precondition has not been met. **The requirements for Sub-exception 1 are:**

(1) The Actor must have a policy that matches the requirements set out above in the Preventing Harm Exception, and the Actor must follow this policy;

(2) If the specific precondition being relied upon is patient consent, the Actor must demonstrate that it has used "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[d] other reasonable assistance to the individual" to obtain the consent; and

(3) The Actor must not encourage or induce the patient to withhold consent.[70]

b. ***Sub-exception 2: Health IT developer of certified Health IT is not covered by HIPAA.*** **This sub-exception only applies to those health IT developers that are not covered by HIPAA. Most health IT developers are business associates of their covered entity customers, so this sub-exception will not apply to them.** ONC recognizes that direct-to-consumer health IT products and services are rapidly growing, and this sub-exception does apply to those Certified HIT Developers.

The specific requirements that must be in place for a Certified HIT Developer to invoke this sub-exception are:

(1) The practice used by the Actor to deny access, use, or exchange of EHI must be included in the Actor's privacy policy. This means that the privacy policy

[68] Final Rule at 25957-58.
[69] Final Rule at 25957.
[70] Final Rule at 25957.

must describe, ***in detail***, the policies and procedures that the Actor will use to decide when the Actor will block access, use, or exchange of EHI with its IT. High-level policies will not comply; they must be detailed.

- Example: A Certified HIT Developer cannot simply say that customer consent is required; it must provide the rationale for why customer consent is reasonable and necessary and how the decision to require consent in a particular instance will be made.

(2) The practice must have been disclosed to the customer in advance. If this disclosure is done through the Certified HIT Developer's customer-facing privacy notice, it must be ***meaningful***, meaning that it must be in **plain language and conspicuous**. The Certified HIT Developer does not have to provide the customer with its organizational privacy policy; a notice will do.

(3) The practice must be "**tailored**" to the privacy risk and implemented in a non-discriminatory way.[71]

c. ***Sub-exception 3: Denying an individual's request for their own information as allowed under 45 CFR 164.524(a)(1) and (2).*** HIPAA allows a covered entity or a business associate to deny an individual access to his/her own PHI in limited situations. These include, but are not limited to, situations in which a licensed healthcare provider determines that providing the PHI would endanger the life or physical safety of the patient or someone else, psychotherapy notes (which are considered the personal notes of the provider), records that are involved in civil litigation, requests by inmates, and certain records involved in clinical trials. **This sub-exception simply says that if an Actor withholds EHI on the basis of this HIPAA provision, it is not violating the Information Blocking rule.**[72]

d. ***Sub-exception 4: Respecting an individual's request to not share information.*** If an individual requests that his/her information not be shared, and an Actor agrees to this request, then the Actor can withhold that information from others, and this will be considered "reasonable and necessary" under the Information Blocking provisions. **The request must:**

(1) Come from the individual;

(2) Be made without any influence or pressure from the covered entity or business associate Actor;

(3) Be documented by the Actor within a "reasonable" time after the request is made; and

[71] Final Rule at 25957.
[72] Final Rule at 25957-58.

(4) Be implemented by the Actor in a consistent and non-discriminatory manner.[73]

ONC observes that this exception is essential to support basic trust and confidence in health IT infrastructure and that without this exception, there would be a "significant risk" that Actors would share EHI in inappropriate circumstances.[74]

[73] Final Rule at 25958.
[74] Final Rule at 25844.

3. <u>Security Exception – When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information not be considered information blocking?</u>[75]

➢ **KEY TAKEAWAY**

The Security Exception allows an Actor to take measures to protect the security of EHI without having to worry that these measures will not be considered "reasonable and necessary" and, thus, in violation of the Information Blocking prohibition.

These Actor's practices must be:

(1) **Directly related** to safeguarding the **confidentiality, integrity, and availability** of EHI;

(2) **Tailored** to **identified** security risks; and

(3) **Implemented consistently** in a **non-discriminatory** manner.[76]

<u>However</u>, **compliance with the HIPAA Security Rule does not guarantee that the Actor meets this exception.**[77] ONC noted in the Proposed Rule that HIPAA establishes minimum security requirements for ePHI, which is a different focus than that of the Security Exception. The purpose of the Security Exception is to provide a flexible approach to promoting the security of EHI, while preventing "unreasonably broad," "onerous," and/or inconsistent measures.[78]

Not every practice taken by an Actor to enhance security is covered by this exception. The practices must meet the following conditions:

(1) The practices must be **directly related to safeguarding the confidentiality, integrity, and availability of EHI**. The key issue is whether the practice is actually necessary and directly related to safeguarding EHI.[79]

(2) The practices must be **tailored to the specific threat being addressed**. The practices, like refusal to exchange EHI with another, cannot be overbroad or extend beyond the duration of the risk.[80]

- In the Proposed Rule, ONC stated that an Actor cannot refuse to transact EHI with a third party designated by an individual just because the Actor does not trust the recipient or has "concerns about what the third party might do with the EHI" (unless falling within the Preventing Harm

[75] Final Rule at 25958.
[76] Final Rule at 25958.
[77] Proposed Rule at 7535-36.
[78] Proposed Rule at 7536.
[79] Final Rule at 25958.
[80] Final Rule at 25958.

Exception).[81] This seems to be a direct reference to healthcare providers not sharing information with third-party apps.

(3) The practices must be **implemented in a consistent and non-discriminatory manner**.[82]

In addition, **if the practice implements an Actor's organizational security policy, the policy must:**

(1) Be in writing;

(2) Address risks that are **specifically identified and assessed**;

(3) Be based on **consensus-based standards or best practices**; and

(4) Contain **objective timelines and other parameters**.[83]

Some practices will not be undertaken pursuant to an organizational security policy because they are unforeseen. **Such practices can meet the Security Exception, but they must be documented, necessary to mitigate the risk and limited to the specific incident being addressed.** Importantly, there also must be "**no reasonable and appropriate alternatives to the practice**" that would address the risk but be less likely to interfere with access, exchange, or use of EHI.[84]

[81] Proposed Rule at 7536.
[82] Final Rule at 25958.
[83] Final Rule at 25958.
[84] Final Rule at 25958.

4. Infeasibility Exception – When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be information blocking?[85]

➢ **KEY TAKEAWAY**

The Infeasibility Exception recognizes that there are real world factors that are beyond an Actor's control and that will prevent the Actor from responding to particular requests for access, exchange, or use of EHI.

Actors may face legitimate practical challenges to complying with a particular request for access, exchange, or use of EHI due to technological capabilities, legal rights, absence of financial resources, or the absence of other means necessary to provide a particular form of access, exchange, or use. ONC also specifically recognizes that, in some cases, an Actor would incur unreasonable costs in order to be able to comply with a specific request.[86]

ONC made substantial revisions to this exception from the version presented in the Proposed Rule in response to comments that it received. For example, ONC abandoned a two-step test that an Actor would have to meet before it could assert that a request for EHI is infeasible. Instead, ONC states that **when an Actor meets one of the conditions listed below *and* the Actor meets the requirement below for responding to requests, the Actor will not be required to fulfill a request for access, exchange, or use of EHI.**

Conditions:

(1) **Uncontrollable events:** These include a natural or human disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunications or internet service interruption, or act of military, civil, or regulatory authority.[87]

(2) **Segmentation:** The Actor cannot "unambiguously segment" the requested EHI from other EHI that:

a. Cannot be accessed, exchanged, or used due to an **individual's preference**; or

b. Cannot be accessed, exchanged, or used under **applicable law**; or

c. May be withheld under the **Preventing Harm Exception**.[88]

[85] Final Rule at 25958.
[86] Final Rule at 25865-66.
[87] Final Rule at 25958.
[88] Final Rule at 25958.

(3) **Infeasible under circumstances:** The Actor demonstrates through written record or other documentation its consistent and non-discriminatory consideration of the following factors that led the Actor to determine that complying with the request would be infeasible under the circumstances:

a. **Type of EHI** and the **purpose for which the EHI may be needed**;

b. **Cost to the Actor** of complying with request;

c. **Financial and technical resources** available to the Actor;

d. Whether the Actor's practice is **non-discriminatory**, and the Actor provides the same access, exchange, or use to all with whom it has business relationships;

e. Whether the **Actor owns or has control over** a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged; *and*

f. Why the Actor was unable to provide access, exchange, or use consistent with the new **Content and Manner Exception**.[89]

Responding to Requests: If an Actor does not fulfill a request, the Actor must provide the reason(s) the request is infeasible to the requestor in writing within ten business days of receipt of the request.[90]

- **NOTE:** In the event the Actor does not respond within 10 business days, it would not meet the exception; however, ONC notes that an Actor's *contemporaneous* documentation about why it could not respond within ten business days could help ONC and OIG identify the Actor's intent in an investigation.[91]
- **NOTE:** The Final Rule does not specify the exact type of information that must be included in the response.[92]

[89] Final Rule at 25958.
[90] Final Rule at 25958.
[91] Final Rule at 25869.
[92] Final Rule at 25958.

5. Health IT Performance Exception – When will an actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information not be considered information blocking?[93]

➢ **KEY TAKEAWAY**

The Health IT Performance Exception recognizes that Actors must occasionally take actions to maintain or improve its IT systems or networks that result in the Actor not being able to fulfill requests for access, exchange, or use of EHI.

An Actor's practice "that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of [EHI] **will not be considered information blocking" *IF* the practice meets one of the following conditions:**

(1) **Maintenance and improvement to health IT.** This will arise when an Actor implements practices for maintenance or improvements that result in the Actor's health IT being temporarily unavailable or temporarily degraded. **The Actor must assure that the practices are:**

a. Implemented to last only as long as necessary;

b. Implemented in a consistent and non-discriminatory manner; and

c. If initiated by an Actor that is *not* a healthcare provider, implemented consistent with existing service level agreements or, if unplanned, as agreed to by the Actor's customer.[94]

(2) **Assured level of performance.** An Actor may take action against a third-party application that is negatively affecting the performance of the Actor's health IT, **provided that:**

a. The action is taken for no longer than necessary to resolve the negative impact;

b. Implemented in a consistent and non-discriminatory manner; and

c. Consistent with existing service level agreements, if applicable.[95]

(3) **Practices that prevent harm.** If the unavailability of an Actor's health IT for maintenance or improvement is "initiated by an actor in response to a risk of harm to a patient or another person," the Actor would need to meet all of the requirements of the Preventing Harm Exception (but not this exception).[96]

[93] Final Rule at 25959.
[94] Final Rule at 25959.
[95] Final Rule at 25959.
[96] Final Rule at 25959.

(4) **Security-related practices.** If the unavailability of an Actor's health IT for maintenance or improvement is implemented to protect against a security risk, the Actor would need to meet all of the requirements of the Security Exception (but not this exception).[97]

[97] Final Rule at 25959.

EXCEPTIONS THAT INVOLVE PROCEDURES FOR FULFILLING REQUESTS TO ACCESS, EXCHANGE, OR USE ELECTRONIC HEALTH INFORMATION

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

➢ **KEY TAKEAWAY**[98]

The Content and Manner Exception reflects the central tenet of Information Blocking according to ONC: Actors should, first and foremost, attempt to fulfill requests to access, exchange, and use EHI in the manner requested.

This is a new exception that ONC added in the Final Rule in response to concerns expressed in comments to the Proposed Rule that the definition of EHI was too broad and to shortcomings of the Infeasibility Exception as that exception was originally proposed. ONC received many comments about the breadth of the proposed definition of EHI and that Actors simply could not comply with the requirement that they fulfill requests for access, exchange, or use of such broadly defined EHI.[99]

ONC observes that this exception is a very high standard and does not permit an Actor to avoid fulfilling a request as requested due to cost burden or similar justification.[100]

If an Actor limits the content of its response to a request for access, exchange, or use of EHI, or the manner in which it responds to such request, the Actor must meet the requirements of the Content Condition and the Manner Condition:

Content Condition: An Actor **must** respond to a request for access, exchange, or use of EHI with, ***at a minimum***:

- **Prior to October 6, 2022:** The **EHI identified by the data elements represented in the USCDI** standard (adopted in § 170.213).
- **On and after October 6, 2022: *All* EHI.**[101]

REMEMBER: ONC also revised the definition of EHI in the Final Rule to align with the definition of ePHI under HIPAA.

[98] Final Rule at 25877.
[99] Final Rule at 25875-76.
[100] Final Rule at 25877.
[101] Final Rule at 25959, as amended by the Interim Final Rule at 70085.

Manner Condition:

(1) **Manner requested.** An Actor **must** fulfill a request (in accordance with the **Content Condition**) in **any manner requested, *unless* the Actor is technically unable**[102] to fulfill the request, **or the Actor cannot reach agreeable terms with the requestor** to fulfill the request.

> ➢ **NOTE: "technically unable" means that the Actor cannot fulfill the request due to technical limitations.**

a. Any fees charged by the Actor in relation to fulfilling the request in any manner requested are not required to satisfy the Fees Exception (discussed next); and

b. Any license of interoperability elements granted by the Actor in relation to fulfilling the request in any manner requested is not required to satisfy the Licensing Exception (discussed later).

(2) **Alternative manner.** If an Actor **does not** fulfill a request (in accordance with the **Content Condition**) in any manner requested because it is **technically unable** to fulfill the request **or cannot reach agreeable terms** with the requestor to fulfill the request, **the Actor must fulfill the request in an alternative manner** and as follows:

a. The Actor **must** fulfill the request **without unnecessary delay and in the following order of priority**, only proceeding to the next manner if the Actor is **technically unable** to fulfill the request in the preceding manner:

(i) Using technology certified under ONC's Health IT Certification Program standards that is specified by the requestor.

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

(A) The Federal Government; or

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

(iii) Using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.

b. Any fees charged by the Actor in relation to fulfilling the request **are** required to satisfy the Fees Exception (discussed next).

c. Any license of interoperability elements granted by the Actor in relation to fulfilling the request **is** required to satisfy the Licensing Exception (discussed later).[103]

[102] Final Rule at 25877.
[103] Final Rule at 25959.

7. Fees Exception – When will an actor's practice of charging fees for accessing, exchanging, or using electronic health information not be considered information blocking?[104]

➢ **KEY TAKEAWAY**

The Fees Exception allows an Actor to charge fees so that it can *recover costs that it reasonably incurs* to develop technologies and provide services that enhance interoperability.

ONC recognizes that an interpretation of the definition of Information Blocking that would prohibit any fee that is likely to interfere with the access, exchange, or use of EHI is likely broader than necessary and could have negative effects on Actors' willingness to invest in the development and dissemination of interoperable technologies and services. **Notably, ONC states that making a profit is not prohibited. Reasonable costs under the exception could include a "reasonable profit,"** provided all applicable conditions are met.[105]

However, the Fees Exception has strict conditions to prevent this exception from being misused. ONC says that "rent seeking, opportunistic fees, and exclusionary practices that interfere with access, exchange, and use of EHI" are prohibited.[106]

What are "reasonably incurred" costs? It DEPENDS on the circumstances!

Fees an Actor charges **must** be:

(1) **Based on objective and verifiable criteria** that are **uniformly applied** across similarly situated persons or entities;

(2) **Reasonably related to the Actor's costs** of providing the type of access, exchange, or use of information;

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

(4) **Based on costs not otherwise recovered** for the same instance of service to a provider and third-party.[107]

Fees an Actor charges **must not** be based on:

(1) Whether the requestor is a **competitor/potential competitor**;

[104] Final Rule at 25959-60.
[105] Final Rule at 25879.
[106] Final Rule at 25879.
[107] Final Rule at 25960.

(2) **Sales, profit, revenue, or other value that the *requestor* or other persons derive or may derive** from the access, exchange, or use of the EHI;

(3) **Costs the Actor incurred due to the health IT being used in non-standard way, *unless*** the requestor agreed to the fees;

(4) Costs associated with **intangible assets**;

(5) **Opportunity costs**; or

(6) Any **costs associated with the creation of intellectual property (IP), *if* the Actor charged a royalty** that included development costs for the IP.[108]

An Actor may charge different prices and impose different payment terms, *but* the **differences must be based on actual differences in costs** that the Actor incurred, **and differences in cost allocation must be based on actual differences in the class of customer**.[109]

> ➢ **NOTE:** The requirement that fees must be reasonably related to the Actor's costs means that Actors must track their costs and use that information to inform their fee setting.

The Final Rule excludes the following costs from protection under the Fees Exception as categorically unreasonable:

(1) Any fees prohibited by HIPAA under 45CFR 164.524(c)(4) (addressing what a covered entity or business associate may and may not charge a patient for access to his/her own information);

(2) A fee based, in any part, on an individual's electronic access to his/her own EHI **or** electronic access by a person or entity designated by the individual;

- Examples: a fee to access a patient portal or charging patient apps a fee to get the patient's EHI

(3) A fee to create a single-patient EHI export[110] or a fee to "export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired."[111]

An Actor must satisfy the Fee Exception conditions, including the methodologies and criteria for determining and allocating costs, with respect to "*each and every* fee" that an Actor charges for access, exchange, or use of EHI.[112] This suggests that **every fee charged that does not meet the requirements of the Fee Exception would be a *separate* violation for purposes of penalties/CMPs**.

[108] Final Rule at 25960.
[109] Final Rule at 25883.
[110] See § 170.315(b)(10).
[111] Final Rule at 25960.
[112] Final Rule at 25888 (emphasis in original).

8. Licensing Exception – When will an actor's practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?[113]

➢ **KEY TAKEAWAY**

The Licensing Exception allows an Actor to license interoperability elements for access, exchange, and use of EHI on *reasonable and non-discriminatory* terms.

Without this exception, ONC believes that the definition of Information Blocking would prevent Actors from charging licensing fees and from refusing to license or disclose interoperability elements.[114]

An Actor's licensing of interoperability elements whereby EHI may be accessed, exchanged, or used must meet the:

(1) Negotiating a License conditions;

(2) Licensing conditions; and

(3) Additional Conditions relating to the provision of interoperability elements.[115]

Negotiating a License Conditions: Upon receiving an *applicable licensing request*, **an Actor must**:

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

(2) **Negotiate a license with the requestor within 30 business days** of receipt of the request, *subject to the **Licensing Conditions** below*.[116]

➢ **NOTE:** We will use the term "*applicable licensing request*" or "*applicable license*" as shorthand for *a request to license interoperability elements for purposes of accessing, exchanging, or using EHI.*

Licensing Conditions: The license provided by the Actor **must**:

(1) **Scope of Rights.** The applicable license must provide **all rights necessary to enable and achieve** the intended access, exchange, or use of EHI.

(2) **Reasonable Royalty.** If the Actor charges a royalty, such royalty must be **reasonable *and***:

a. It must be **non-discriminatory**;

[113] Final Rule at 25960-61.
[114] Final Rule at 25888.
[115] Final Rule at 25960.
[116] Final Rule at 25960.

b. It must be based "solely on the **independent value** of the actor's technology to the licensee's products and **not on any strategic value stemming from the actor's control** over essential means of accessing, exchanging, or using [EHI]";[117] and

c. It must not include a royalty for intellectual property (IP), *if* the Actor recovered any development costs for the IP under the Fees Exception.

In addition: If applicable, an Actor that has licensed the interoperability elements through a standards-developing organization in accordance with that organization's licensing policies on terms consistent with the Licensing Exception may charge a royalty consistent with those policies.

(3) **Non-Discriminatory Terms.** All of the terms on which the Actor licenses or otherwise provides the interoperability elements must be non-discriminatory ***and***:

a. **Must be based on "objective and verifiable criteria that are uniformly applied** for all similarly situated classes of persons and requests"; and

b. **Must NOT be based on:**

(i) Any **anti-competitive** interests; or

(ii) **Any revenue or other value the requestor may derive** from the applicable license.

(4) **Collateral Terms.** An Actor **must not** require the licensee to:

a. **Refrain from competing** with the Actor;

b. **Deal exclusively** with the Actor;

c. **Obtain additional licenses, products, or services** that are unrelated **OR** that could be unbundled from the applicable license;

d. **Convey any interest** in any of the licensee's IP to the Actor; or

e. **Pay any fee other than the Reasonable Royalty** (described above) unless such practice falls within the **Fees Exception**.

(5) **Non-Disclosure Agreement (NDA).** An Actor **may** require the licensee to enter into a **reasonable** NDA to protect the Actor's ***trade secrets*** ***if*** the NDA states—***with particularity***—all information claimed as a trade secret.[118]

> ➢ **NOTE:** The information for which protection is sought under the NDA **must meet the definition of a "*trade secret*" under applicable law**.

[117] Final Rule at 25960 (emphasis added).
[118] Final Rule at 25961.

Additional Conditions: Finally, Actors **must not engage in any practice that has the purpose or effect** of any of the following with respect to the applicable license (quoted in their entirety):

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

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

(3) **Degrading the performance or interoperability** of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.[119]

[119] Final Rule at 25961 (emphasis added).

LET'S RECAP OUR KEY TAKEAWAYS:

Information Blocking Takeaways

- **Information Blocking** is a **practice** that an **Actor knows or**, *in some cases*, **should know** is **likely to interfere** with **access**, **exchange**, or **use** of **electronic health information ("EHI")**.

- For purposes of the Information Blocking restrictions, **Actors** are (1) **Healthcare Providers**, (2) **Health IT Developers of Certified Health IT**, and/or (3) **Health Information Networks (HINs)** and **Health Information Exchanges (HIEs)**.

- A **health IT developer of certified health IT** is (1) an **individual or entity** (2) that **develops or offers Health Information Technology** (3) ***AND*** has **health information technology certified** under ONC's Health IT Certification Program (4) **at the time such individual or entity engages in a "practice"** that is the subject of an Information Blocking claim.

- ONC applies a functional definition of a **health information network (HIN) or health information exchange (HIE)** (provided below) that focuses on what an **individual or entity** actually **does**, **or has the authority to do**, rather than on how it is organized, what it is called, or what type of legal entity it is.

  

  The definition is **extremely** broad, and there are likely organizations that do not consider themselves HINs/HIEs that will fall within this functional definition.

- **All Actors must be extremely careful in evaluating their risk profile for Information Blocking and carefully consider every aspect of how they deal with EHI, especially with respect to requests for access, exchange, or use of EHI. Actors must think about their risk of Information Blocking very expansively and think about both the actions they take *AND* the actions that they fail to take.**

- ONC states that **a practice is likely to interfere "if, under the circumstances, there is a reasonably foreseeable risk that the practice will interfere with access, exchange, or use of EHI."**

Exceptions Takeaways

- **To meet an exception, the Actor must demonstrate that it met *ALL* of the requirements of the applicable exception. Meeting *most* of the requirements of an exception (or a combination of partial requirements from different exceptions) is NOT sufficient to fit within the safe harbor of an exception.**
- **The Preventing Harm Exception is intended to "allow for the protection of patients and other particular persons against substantial risk of harm" that may arise from access, exchange, or use of EHI in defined circumstances.**
- **The Privacy Exception is intended to "allow for the protection of patients and other particular persons against substantial risk of harm" that may arise from access, exchange, or use of EHI in defined circumstances.**
- **The Security Exception allows an Actor to take measures to protect the security of EHI without having to worry that these measures will not be considered "reasonable and necessary" and, thus, in violation of the Information Blocking prohibition.**
- **The Infeasibility Exception recognizes that there are real world factors that are beyond an Actor's control and that will prevent the Actor from responding to particular requests for access, exchange, or use of EHI.**
- **The Health IT Performance Exception recognizes that Actors must occasionally take actions to maintain or improve its IT systems or networks that result in the Actor not being able to fulfill requests for access, exchange, or use of EHI.**
- **The Content and Manner Exception reflects the central tenet of Information Blocking according to ONC: Actors should, first and foremost, attempt to fulfill requests to access, exchange, and use EHI in the manner requested.**
- **The Fees Exception allows an Actor to charge fees so that it can *recover costs that it reasonably incurs* to develop technologies and provide services that enhance interoperability.**
- **The Licensing Exception allows an Actor to license interoperability elements for access, exchange, and use of EHI on *reasonable and non-discriminatory* terms.**

Information Blocking Bootcamp 2020
Information Blocking Summary

APPENDIX 1

ONC's List of 42 Examples of Specific Activities from the Proposed Rule that *Could* Constitute a Practice Resulting in an Information Blocking Violation

1. Formal restrictions through contract or license terms, EHI access policies, organizational policies and procedures, or other instruments or documents that relate to EHI or health IT
2. Exercising IP rights or other rights
3. Health system policy requiring consent to exchange EHI for treatment even though not required by law
4. EHR developer refuses to share technical information needed to export data
5. HIN restriction on end-user sharing of EHI with non-HIN members
6. Health system citing HIPAA as a reason that it cannot share EHI when that it not the case
7. EHR vendor only provides EHI in PDF format upon termination of an agreement with a customer
8. An EHR developer sues to prevent a clinical data registry from providing interfaces to physicians who use the developer's EHR technology and wish to submit EHI to the registry. The EHR developer claims that the registry is infringing the developer's copyright in its database because the interface incorporates data mapping that references the table headings and rows of the EHR database in which the EHI is stored.
9. A health IT developer of certified health IT refuses to license interoperability elements that are reasonably necessary for the developer's customers, their IT contractors, and other health IT developers to develop and deploy software that will work with the certified health IT.
10. An EHR developer ostensibly allows third-party developers to deploy apps that are interoperable with its EHR system. However, as a condition of doing so, the third-party developers must provide their source code and grant the EHR developer the right to use it for its own purposes—terms that almost no developer would willingly accept.
11. Disabling or restricting the use of a capability that enables users to share EHI with users of other systems or to provide access to EHI to certain types of persons or for certain purposes that are legally permissible.
12. An actor configures or otherwise implements technology in ways that limit the types of data elements that can be exported or used from the technology.
13. Configuring capabilities in a way that removes important context, structure, or meaning from the EHI, or that makes the data less accurate, complete, or usable for important purposes for which it may be needed.

14. Implementing capabilities in ways that create unnecessary delays or response times, or that otherwise limit the timeliness of EHI accessed or exchanged.

15. An actor deploys technological measures that limit or restrict the ability to reverse engineer the functional aspects of technology in order to develop means for extracting and using EHI maintained in the technology.

16. A health system implements locally-hosted EHR technology certified to proposed § 170.315(g)(10) (the health system acts as an API Data Provider as defined by § 170.102). As required by proposed § 170.404(b)(2), the technology developer provides the health system with the capability to automatically publish its production endpoints (i.e., the internet servers that an app must "call" and interact with in order to request and exchange patient data). The health system chooses not to enable this capability, however, and provides the production endpoint information only to apps it specifically approves. This prevents other applications—and patients that use them—from accessing data that should be made readily accessible via standardized APIs.

17. A hospital directs its EHR developer to configure its technology so that users cannot easily send electronic patient referrals and associated EHI to unaffiliated providers, even when the user knows the Direct address and/or identity (i.e., National Provider Identifier) of the unaffiliated provider.

18. An EHR developer that prevents (such as by way of imposing exorbitant fees unrelated to the developer's costs, or by some technological means) a third-party clinical decision support (CDS) app from writing EHI to the records maintained by the EHR developer on behalf of a health care provider (despite the provider authorizing the third-party app developer's use of EHI) because the EHR developer: (1) offers a competing CDS software to the third-party app; and (2) includes functionality (e.g., APIs) in its health IT that would provide the third party with the technical capability to modify those records as desired by the health care provider.

19. Although an EHR developer's patient portal offers the capability for patients to directly transmit or request for direct transmission of their EHI to a third party, the developer's customers (e.g., health care providers) choose not to enable this capability.

20. A health care provider has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient's health care provider but takes several days to respond.

21. A health IT developer of certified health IT refuses to license an API's interoperability elements, to grant the rights necessary to commercially distribute applications that use the API's interoperability elements, or to provide the related services necessary to enable the use of such applications in production environments.

22. An EHR developer of certified health IT requires third-party applications to be "vetted" for security before use but does not promptly conduct the vetting or conducts the vetting in a discriminatory or exclusionary manner.

23. A health IT developer of certified health IT refuses to license interoperability elements that other software applications require to efficiently access, exchange, and use EHI maintained in the developer's technology.

24. An EHR developer of certified health IT maintains an "app store" through which other developers can have "apps" listed that run natively on the EHR developer's platform. However, if an app "competes" with the EHR developer's apps or apps it plans to develop, the developer *requires* that the app developer grant the developer the right to use the app's source code.

25. A health care provider engages a systems integrator to develop an interface engine. However, the provider's license agreement with its EHR developer prohibits it from disclosing technical documentation that the systems integrator needs to perform the work. The EHR developer states that it will only permit the systems integrator to access the documentation if all of its employees sign a broad non-compete agreement that would effectively bar them from working for any other health IT companies.

26. An EHR developer of certified health IT maintains an "app store" through which other developers can have "apps" listed that run natively on the EHR developer's platform. The EHR developer charges app developers a substantial fee for this service unless an app developer agrees not to deploy the app in any other EHR developers' app stores.

27. A hospital is working with several health IT developers to develop an application that will enable ambulatory providers who use different EHR systems to access and update patient data in the hospital's EHR system from within their ambulatory EHR workflows. The inpatient EHR developer, being a health IT developer of certified health IT, pressures the hospital to abandon this project, stating that if it does not it will no longer receive the latest updates and features for its inpatient EHR system.

28. A health IT developer of certified health IT discourages customers from procuring data integration capabilities from a third-party developer, claiming that it will be providing such capabilities free of charge in the next release of its product. In reality, the capabilities it is developing are more limited in scope and are still 12-18 months from being production-ready.

29. A health system insists that local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and facilities. The health system threatens to revoke admitting privileges for physicians that do not comply.

30. An HIN charges additional fees, requires more stringent testing or certification requirements, or imposes additional terms for participants that are competitors, are potential competitors, or may use EHI obtained via the HIN in a way that facilitates competition with the HIN.

31. A health care provider imposes one set of fees and terms to establish interfaces or data sharing arrangements with several registries and exchanges but offers another costlier or significantly onerous set of terms to establish substantially similar interfaces and

arrangements with an HIE or HIN that is used primarily by health plans that purchase health care services from the provider at negotiated reduced rates.

32. A health IT developer of certified health IT charges customers fees, throttles speeds, or limits the number of records they can export when exchanging EHI with a regional HIE that supports exchange among users of competing health IT products but does not impose like fees or limitations when its customers exchange EHI with enterprise HIEs that primarily serve users of the developer's own technology.

33. As a condition of disclosing interoperability elements to third-party developers, an EHR developer requires third-party developers to enter into business associate agreements with all of the EHR developer's covered entity customers, even if the work being done is not for the benefit of the covered entities.

34. A health IT developer of certified health IT takes significantly longer to provide or update interfaces that facilitate the exchange of EHI with users of competing technologies or services.

35. Certain practices that artificially increase the cost and expense associated with accessing, exchanging, and using EHI will implicate the information blocking provision. An actor may seek to extract profits or capture revenue streams that would be unobtainable without control of a technology or other interoperability elements that are necessary to enable or facilitate access, exchange, or use of EHI.

36. An EHR developer of certified health IT charges customers a fee to provide interfaces, connections, data export, data conversion or migration, or other interoperability services, where the amount of the fee exceeds the actual costs that the developer reasonably incurred to provide the services to the particular customer(s).

37. An EHR developer of certified health IT charges a fee to perform an export using the EHI export capability proposed in § 170.315(b)(10) for the purposes of switching health IT systems or to provide patients access to EHI.

38. An EHR developer of certified health IT charges more to export or use EHI in certain situations or for certain purposes, such as when a customer is transitioning to a competing technology or attempting to export data for use with a HIE, third-party application, or other technology or service that competes with the revenue opportunities associated with the EHR developer's own suite of products and services.

39. An EHR developer of certified health IT interposes itself between a customer and a third-party developer, insisting that the developer pay a licensing fee, royalty, or other payment in exchange for permission to access the EHR system or related documentation, where the fee is not reasonably necessary to cover any additional costs the EHR developer incurs from the third-party developer's activities.

40. An analytics company provides services to the customers of an EHR developer of certified health IT, including de-identifying customer EHI and combining it with other data to identify areas for quality improvement. The EHR developer insists on a revenue sharing arrangement whereby it would receive a percentage of the revenue generated from these

activities in return for facilitating access to its customers' EHI, which turns out to be disadvantageous to customers. The revenue the EHR developer would receive exceeds its reasonable costs of facilitating the access to EHI.

41. An EHR developer of certified health IT implements the C-CDA for receiving transitions of care summaries but only sends transitions of care summaries in a proprietary or outmoded format.

42. A health IT developer of certified health IT adheres to the "required" portions of a widely adopted industry standard but chooses to implement proprietary approaches for "optional" parts of the standard when other interoperable means are readily available.

The Office of the National Coordinator for Health Information Technology

CURES ACT FINAL RULE

Changes and Clarifications from the Proposed Rule to the Final Rule

Changes and Clarifications Related to the ONC Health IT Certification Program

Electronic Health Information (EHI) Export Certification Criterion

PROPOSED RULE

We proposed to adopt a new 2015 Edition certification criterion, referred to as "EHI Export," in § 170.315(b)(10). The criterion's proposed conformance requirements were intended to provide a means to export the entire EHI that a certified health IT product produces and electronically manages to support two contexts: (1) single patient EHI export; and (2) patient EHI export when a health care provider is switching health IT systems.

FINAL RULE

- The final certification criterion and scope of data that a Health IT Module certified to § 170.315(b)(10) must export is more specific ("at the time of certification") and aligned to the definition of "EHI" finalized in § 171.102 (see the *EHI definition* section below).
- Consistent with the "Assurances" Condition of Certification, developers of certified health IT whose Health IT Modules need to be certified to § 170.315(b)(10) must do so and provide such capabilities to their customers within 36 months of the final rule's publication date (compared to 24 months as proposed).

FHIR Standard for Application Programming Interface (API) Certification Criterion

PROPOSED RULE

We proposed to adopt the HL7® Fast Healthcare Interoperability Resources® (FHIR®) standard as a foundational standard and requested comment on four options to determine the best version of FHIR® to adopt.

FINAL RULE

We have adopted FHIR Release 4.

Communications Condition and Maintenance of Certification – Permitted Restrictions for Intellectual Property and Visual Communications

PROPOSED RULE

We proposed to prohibit health IT developers from restricting the sharing of screenshots of their health IT, except in limited circumstances. We also proposed that health IT developers would not be permitted to prohibit or restrict, or purport to prohibit or restrict, communications that would be a "fair use" of any copyright work comprised in the developer's health IT.

Changes and Clarifications Related to the ONC Health IT Certification Program

FINAL RULE

- We clarified in the final rule that screenshots are only one form of visual communications protected under the Cures Act, and that the protections afforded to screenshots in the Communications Condition of Certification extend to video. Such visual communications are critical to addressing issues with health IT related to patient safety, usability, security, and interoperability.
- Developers may, under the permitted prohibitions and restrictions section of the condition, restrict communications that involve intellectual property, provided that -
  - Any prohibition or restriction imposed by a developer must be no broader than necessary to protect the developer's intellectual property; and
  - Are consistent with the other requirements of this section.
- Developers must not restrict or preclude a public display of a portion of a work subject to copyright protection (without regard to whether the copyright is registered) that would reasonably constitute a "fair use" of that work.
- Developers may limit the sharing of screenshots and video of their health IT products to only the relevant number of screenshots and amount of video needed to communicate about the certified health IT products regarding one or more of the six protected subject areas identified in the 21st Century Cures Act. Developers may limit the sharing of videos to only those videos that address temporal matters that cannot be communicated through screenshots or other forms of communication.

Changes and Clarifications Related to Information Blocking

Compliance Timeline

PROPOSED RULE

The information blocking provision did not specify any delays in implementation once finalized.

FINAL RULE

Health care providers, health IT developers of certified health IT, health information exchanges, and health information networks ("actors") do not have to comply with the information blocking provision until six months after publication of the final rule. ONC and OIG are also coordinating timing of the compliance date and the start of information blocking enforcement. Enforcement of information blocking civil monetary penalties (CMPs) in section 3022(b)(2)(A) of the PHSA will not begin until established by future notice and comment rulemaking by OIG. As a result, actors would not be subject to penalties until CMP rules are final. At a minimum, the timeframe for enforcement would not begin sooner than the compliance date of the ONC final rule and will depend on when the CMP rules are final. Discretion will be exercised such that conduct that occurs before that time will not be subject to information blocking CMPs.

Changes and Clarifications Related to Information Blocking

EHI Definition

PROPOSED RULE

The information blocking provision applies to "EHI," which is not defined in the Cures Act. We proposed a broad definition of EHI in the proposed rule.

FINAL RULE

- We focused the scope of EHI in § 171.102 in the final rule to mean electronic protected health information (ePHI) as the term is defined for HIPAA 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 (other than psychotherapy notes as defined in 45 CFR 164.501 or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding), regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103.
- We also clarify that until 24 months after the publication date of the final rule, EHI for purposes of the information blocking definition is limited to the EHI identified by the data elements represented in the USCDI standard adopted in § 170.213.

Access, Exchange, and Use Definitions

FINAL RULE

We clarified the definitions of **access, exchange, and use** in the final rule. For example, we finalized "use" to mean the ability for EHI, **once accessed or exchanged**, to be understood and acted upon. We also emphasized that "transmitted" within the definition of "exchange" is not limited to a one-way transmission, but instead is inclusive of all transmissions.

What it Means to "Interfere with" Access, Exchange, or Use of EHI

FINAL RULE

- Provided certain criteria are met, we clarified in the final rule that it would **not** be considered an "interference with" the access, exchange, or use of EHI (and thus **not** "information blocking") if an information blocking "actor" engaged in practices to educate patients about the privacy and security risks posed by the apps they choose to receive their EHI.
- 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 as to whether the third party's privacy policy and practices (including security practices) meet certain "best practices" set by the market for privacy policies and practices.
- We recommended that the privacy policies and practices of third-party apps should, at a minimum, adhere to the following:
  - The privacy policy is made publicly accessible at all times, including updated versions;
  - The privacy policy is shared with all individuals that use the technology prior to the technology's receipt of EHI from an actor;
  - The privacy policy is written in plain language and in a manner calculated to inform the individual who uses the technology;

Changes and Clarifications Related to Information Blocking

- 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
- 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 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).

- We clarified in the final rule that the information blocking provision does not require actors to violate business associate agreements or associated service level agreements. However, we also clarified that such agreements *could* constitute an interference if used in a discriminatory manner by an actor to limit or prohibit the access, exchange, or use of EHI for treatment purposes that otherwise would be permitted by the Privacy Rule.

Health Information Network (HIN) and Health Information Exchange (HIE) Definitions

PROPOSED RULE

The terms "network" and "exchange" are not defined in the Cures Act. ONC proposed functional definitions for these "actors" under the information blocking provision that focused on the role of the actors in the health information ecosystem.

FINAL RULE

We focused the HIN and HIE definitions in four ways:

1. Combined the definitions of HIN and HIE to create one functional definition that applies to both statutory terms in order to clarify the types of individuals and entities that would be covered.
2. Limited the types of actions that would be necessary for an actor to meet the definition of HIN or HIE.
3. Revised the definition to specify that to be a HIN or HIE there must be more than two unaffiliated individuals or entities besides the HIN/HIE that are enabled to exchange with each other.
4. Focused the definition's scope to be about exchange related to treatment, payment, and health care operations, as each are defined in the HIPAA Rules.

Structure of the Exceptions

PROPOSED RULE

We proposed seven categories of practices that would be exceptions to the information blocking definition.

FINAL RULE

We finalized eight information blocking exceptions, including the new Content and Manner Exception (discussed below). We restructured the exceptions into two categories:

- Exceptions that involve not fulfilling requests to access, exchange, or use EHI; and
- Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.

Changes and Clarifications Related to Information Blocking

Promoting Privacy Exception

PROPOSED RULE

We proposed that to qualify for this exception when individual consent or authorization is a precondition to providing access, exchange, or use of EHI, an actor would need to do all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization.

FINAL RULE

To qualify for this exception when individual consent or authorization is a precondition to providing access, exchange, or use of EHI, an actor must have used reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all applicable requirements or have provided other reasonable assistance with respect to the deficiencies. In effect, this places more of an obligation on the party requesting the EHI and the individual to attempt to satisfy the precondition by providing a consent or authorization.

New Content and Manner Exception

FINAL RULE

The Content and Manner Exception was not explicitly proposed in the proposed rule though many of its principles were addressed in various ways. This new exception addresses a broad range of comments we received about the required content and manner of an actor's response to a request to access, exchange, or use EHI. Under the exception, it will not be information blocking for an actor to limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided certain conditions are met. This exception supports innovation and competition by allowing actors to first attempt to reach and maintain market negotiated terms for the access, exchange, and, use of EHI.

- Content Condition establishes the content (EHI) an actor must provide in response to a request to access, exchange, or use EHI in order to satisfy the exception.
  1. Up to 24 months after the publication date of the Cures Act final rule, an actor must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard.
  2. On and after 24 months after the publication date of the Cures Act final rule, an actor must respond to a request to access, exchange, or use EHI with EHI as defined in § 171.102.
- **Manner Condition** establishes the manner in which an actor must fulfill a request to access, exchange, or use EHI in order to satisfy this exception.
  - » An actor may need to fulfill a request in an alternative manner when the actor is:
    - Technically unable to fulfill the request in any manner requested; ***or***
    - Cannot reach agreeable terms with the requestor to fulfill the request.
  - » If an actor fulfills a request in an alternative manner, such fulfillment must comply with the order of priority described in the manner condition and must satisfy the Fees Exception and Licensing Exception, as applicable.

Changes and Clarifications Related to Information Blocking

Infeasibility Exception

FINAL RULE

- We restructured the exception to include:
  - » Two new discreet conditions concerning:
    - Uncontrollable events; and
    - Inability to unambiguously segment the requested EHI.
  - » A condition that describes factors that will be considered to determine whether a request is infeasible under the circumstances.
- We removed the "reasonable alternative" requirement from this exception and repurposed that concept in the new Content and Manner Exception (see above). The Content and Manner Exception improves on the "reasonable alternative" requirement in the proposed rule by clarifying actors' obligations for providing access, exchange, or use of EHI in *all* situations, creating actionable technical procedures, and aligning the requirement for providing an alternative with the Fees Exception and Licensing Exception.

Fees Exception – Profits

FINAL RULE

We reiterated and included in regulation text that actors may charge fees, **including fees that result in a reasonable profit margin**, for accessing, exchanging, or using EHI. We also clarified how the Fees Exception works with the Licensing Exception and Content and Manner Exception.

Licensing Intellectual Property

FINAL RULE

We reiterated and clarified in the final rule that an actor does not need to license its interoperability elements if the actor is able to fulfill a request to access, exchange, or use EHI in an alternative manner without licensing its IP (see the Content and Manner Exception discussed above). We also clarified how the Licensing Exception works with the Fees Exception and Content and Manner Exception.