GUIDE TO INFORMATION BLOCKING[1]

By: Michael Bossenbroek[2]

[1] This publication is intended to serve as a preliminary research tool for attorneys for educational purposes only. It should not be used as the sole basis for making critical business or legal decisions. This publication does not constitute, and should not be relied upon as, legal advice.

[2] Michael Bossenbroek Senior Counsel at Corewell Health. He provides legal counsel on a wide range of hospital operations matters that include including physician contracting, Stark and Anti-Kickback Statute compliance, patient privacy and HIPAA, behavioral and mental health, laboratory, pharmacy, 340B, and information technology. Mr. Bossenbroek is an active member of the State Bar of Michigan's Health Care Law Section. He has spoken and written on health care law topics for the ABA, AHLA, the State Bar of Michigan, and other organizations.

TABLE OF CONTENTS

INTRODUCTION

The purpose of this White Paper is to provide a roadmap for compliance with the 21st Century Cures Act Information Blocking Rule ("Rule"). This White Paper will begin by briefly outlining the regulatory history of the Rule. It will then describe the basics of the Information Blocking Rule by (1) defining the parties subject to Information Blocking, (2) identifying and defining the key terms in the Rule, (3) describing the elements of an Information Blocking violation, (4) outlining the nine (9) exceptions to the Information Blocking Rule, and (5) discussing enforcement and penalties of the Rule. This White Paper will also discuss additional considerations related to enforcement, the Rule's relationship to other federal and state laws, and highlight some practical operational and compliance considerations around the Information Blocking Rule.

I. What is Information Blocking?

A. Regulatory History of the Information Blocking Rule

1. The 21st Century Cures Act

On December 13, 2016, President Obama signed into law the 21st Century Cures Act (the "Cures Act").[1] Among the many provisions included in the bill, the Cures Act amended the Public Health Service Act to prohibit "Information Blocking."[2] Section 3022 broadly prohibits practices that the statute defines as "Information Blocking" and authorized the Secretary of Health and Human Services ("HHS") to promulgate rules to identify reasonable and necessary activities that do not constitute Information Blocking. The Office of the National Coordinator for Health Information Technology (ONC) is the agency within HHS charged with the responsibility of implementing the key provisions of the Cures Act relating to interoperability, including Information Blocking.[3]

2. Information Blocking Proposed and Final Rules

On March 4, 2019, ONC published a Proposed Rule for Information Blocking, that among other things, proposed eight exceptions to the broad Information Blocking prohibition, and proposed definitions of various statutory terms.[4] Following notice and comment, ONC published the Final Rule on May 1, 2020.[5] The Final Rule originally established a compliance date of November 2, 2020. However, due to the COVID pandemic, ONC subsequently extended the compliance date to April 5, 2021.[6]

Since the publication of the Final Rule on May 1, 2020, ONC and OIG have engaged in additional rulemaking. On July 3, 2023, OIG published a final rule authorizing civil monetary penalties (CMPs) for Information Blocking.[7] On November 1, 2023, CMS and ONC published a proposed rule to establish disincentives for certain health care providers that engage in Information Blocking.[8] This proposed rule was finalized on July 1, 2024.[9] ONC published the Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing final rule ("HTI-1") on January 9, 2024, which updated and amended provisions of the Information Blocking rule by, among other things, adding a ninth exception to Information Blocking.[10]

B. What is Information Blocking?

The Rule defines Information Blocking is a practice[11] by an Actor[12] that is likely to interfere with access,[13] exchange,[14] or use[15] of electronic health information ("EHI"), unless that practice is either (1) required by law, or (2) covered by one of nine exceptions to Information Blocking granted in the Information Blocking Rule.[16] Unlike HIPAA, which generally speaking prohibits disclosure of protected health information, the Rule requires granting a request to use, disclose, or access of EHI unless an

exception applies. At the risk of overstating the case, the Rule introduces a paradigm shift from "thou shalt not" to "thou shalt" share the requested information.

Given this definition of Information Blocking, a series of questions must be answered to determine if a particular "practice" constitutes Information Blocking:

1. Is the individual or entity engaging in the practice an "Actor" as defined in 45 CFR 171.102;
2. Does the claim involve "EHI" as defined in 45 CFR 171.102;
3. Does the practice rise to the level of interference with access, exchange, or use of EHI;
4. Is the practice required by law;
5. Does the practice meet one of the nine exceptions under 45 CFR 171;
6. Did the Actor act have the required standard of knowledge?

These questions provide a helpful roadmap to the Information Blocking rule. Each of these questions will be explored in more detail in the following sections.

COMPLIANCE TIP: If the answers to questions 1-3 and 6 is "yes" and questions 4 and 5 are "no" it is likely that the Actor has engaged in a practice that constitutes Information Blocking.

1. What "Actors" Are Subject to the Rule?

The Rule defines four categories of Actors — individuals and entities — that are subject to the Rule. These Actors are (1) "health care providers," (2) "health IT developers of certified health IT," (3) "health information exchanges," and (4) "health information networks."[17] For purposes of the Final Rule, "health information exchanges" and "health information networks" are treated the same.

The first category of Actor, a "health care provider," is not defined by statute. Consequently, it is broadly defined by reference to the statutory definition of "health care provider" found at 42 USC 300jj.[18] Health care provider includes hospitals, skilled nursing facilities, physicians, and advanced practice providers.[19]

The second category of Actor is a "health IT developer of certified health IT."[20] These are individuals or entities that develop or offer health information technology[21] and which have one or more Health IT Modules certified under the ONC Health IT Certification Program.[22] A health care provider that self-develops health IT that is not offered for others is not a "health IT developer of certified health IT." The phrases "offer health information" or "offer health IT" are defined extensively by ONC to "hold out for sale, resale, license, or relicense or sell, resell, license, relicense or otherwise provide or supply health information technology" where such health information technology includes one or more Health IT Modules.[23] ONC's definition carves out several activities and arrangements, such as (1) donation and subsidized supply arrangements that consist of only funding, (2) implementation and use activities such as issuing user accounts or login credentials to employees or contractors, and (3) certain consulting, legal, and operations management arrangements that require access to or providing of CEHRT.[24] These activities are not considered examples of offering health IT.

ONC in its commentary warned that the exclusion of "self-developed" health IT would not be available if the health care provider offers or supplies its self-developed health IT to another entity for that entity's use in its own independent operation.[25] For example, it is possible for a health care provider to also be a health IT developer of certified health IT. If the provider manages an EHR Donation program that consists of more than providing funding to subsidize the program, it will also meet the definition of a health IT developer of certified health IT.

The third and fourth types of Actors, treated together by the Rule, are a "health information exchange" and a "health information network."[26] They are an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information: (1) among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other and (2) that is for a treatment, payment, or health care operations purpose as defined by HIPAA, regardless whether the individuals or entities are subject to the requirements of HIPAA in Parts 160 and 164.[27]

COMPLIANCE TIP: Because ONC views the definition of Actor to be based on function, take time to understand what type of Actor an individual or entity might be, and understand the requirements and potential fines and penalties associated with that type of entity.

2. Is Electronic Health Information (EHI) at issue?

Electronic health information (EHI) is a new definition created by the Rule.[28] It is closely related to the definition of electronic protected health information (ePHI)[29] under HIPAA, but the two terms are not synonymous. EHI is defined as the ePHI that is included in an entity's designated record set.[30] EHI excludes (1) psychotherapy notes as defined under HIPAA and (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[31] EHI also does not include the paper records of an Actor.

COMPLIANCE TIP: Because the definition of EHI borrows heavily from the terms ePHI and designated record set as defined by HIPAA, an entity should review the ePHI it maintains and how it defines its designated record set. If one does not already exist, consider creating a policy that defines the entity's designated record set.

3. Does the practice rise to the level of interference with access, exchange, or use of EHI?

The Rule prohibits an Actor from a practice that interferes with the access, exchange, or use of EHI.[32] It defines "interfere with" or "interference" to mean "prevent, materially discourage, or otherwise inhibit."[33] In an attempt to give some idea of what that means in practice, ONC in its commentary to the Final Rule gave a non-exhaustive list of hypothetical practices that, in its view, likely would interfere with access, exchange or use of EHI. However, ONC cautioned that "any analysis of Information Blocking necessarily requires a careful consideration of the individual facts and circumstances."[34]

ONC divided these illustrative examples into two categories: (1) formal restrictions, such as organizational policies and contract terms, and (2) informal practices such as an Actor's refusal to exchange or provide access to EHI, ignoring requests for EHI, giving implausible reasons for denying requests, or requiring objectively unreasonable terms.[35] ONC provided illustrative examples that it further broke down into more descriptive categories. These examples include practices that:

- Restrict access, exchange, or use by:

  - Negotiating contracts and agreements with unconscionable terms or that exploit unequal bargaining power related to accessing, exchanging, and using EHI;[36]
  - Using BAAs in a discriminatory manner;[37]

- Limit or restrict the interoperability of health IT by disabling or restricting the use of capabilities that enable sharing of EHI; limiting the types of data elements that can be exported or used; rendering the data less accurate, complete, or usable;[38] by:

    - Withholding a FHIR[39] service base URL;[40]
    - Refusing to register a software application that enables a patient to access their EHI;[41]

- Impede innovations and advancements in access, exchange, or use of health IT[42] by:

    - Refusing to license or allow the disclosure of interoperability elements
    - Restricting use of interoperability elements

- Rent seeking and other opportunistic pricing practices;[43]
- Implement non-standard practices that substantially increase the complexity or burden of accessing, exchanging, or using EHI;[44]

In sum, the scope of practices, formal and more informal, that may constitute Information Blocking is extremely broad. An Actor must carefully evaluate its existing practices to consider to what extent it may be engaging in Information Blocking and whether that practice is otherwise permitted by an exception.

COMPLIANCE TIP: Considering the broad definition of a practice, an Actor should take an expansive view of its formal and informal restrictions regarding the access, use, and exchange of its EHI when considering whether the restriction would be considered an interfering practice.

4. Is the Practice Required by Law?

Practices that are "required by law" are not Information Blocking.[45] Neither the statute nor the Rule specifically define when a practice is "required by law." However, ONC in its Preamble to the Proposed and Final Rules offered more detail about the meaning of this phrase.[46] ONC distinguished, first of all, between a practice that is <u>required</u> by law and a practice that is <u>permitted</u> by law. Only those practices that are explicitly required by law are exempt from the Information Blocking rules. Practices that are permitted under a state or federal law may still implicate the Rule and, if it otherwise constitutes Information Blocking, would be required to meet an exception.

In its commentary, ONC also provided more detail about what types of laws would qualify under this category. It clarified that the phrase "by law" refers to federal and state laws, including "statutes, regulations, court orders, and binding administrative decisions or settlements, such as (at the Federal level) those from the FTC or the Equal Employment Opportunity Commission (EEOC)."[47] It also includes tribal laws where applicable.

5. Does the Practice Fall within an Exception to Information Blocking?

In the Final Rule, ONC originally published eight exceptions to the Information Blocking Rule.[48] The HTI-1 Final Rule added a ninth exception. ONC determined that each of these exceptions protected practices that were reasonable and necessary to further the underlying public policies of Information Blocking.[49] Therefore, a practice will not be treated as Information Blocking if the Actor satisfies each of the elements of one of these nine exceptions.[50] In the absence of an Actor satisfying one of these exceptions, a practice may constitute Information Blocking.

The nine exceptions are divided into three categories, corresponding to Subparts B, C, and D in the Information Blocking rule. The first category consists of five exceptions that apply where the Actor

does not fulfill requests to access, exchange, or use EHI.[51] These exceptions are the (1) Preventing Harm Exception,[52] (2) Privacy Exception,[53] (3) Security Exception,[54] (4) Infeasibility Exception,[55] and (5) Health IT Performance Exception.[56] The second category consists of three exceptions that may apply where the Actor is fulfilling requests to access, exchange or use EHI, but may impose conditions on the request or fulfill them in a different manner.[57] These three exceptions are the (1) Manner Exception,[58] (2) Fees Exception,[59] and (3) Licensing Exception.[60] ONC created a separate category for the ninth exception related to participation in the Trusted Exchange Framework Common Agreement ("TEFCA").

(a) Subpart B - Exceptions That Involve Not Fulfilling Requests to Access, Exchange, or Use Electronic Health Information

(i) Preventing Harm Exception

ONC created the Preventing Harm Exception to permit certain practices that are reasonable and necessary to prevent specific types of harm to a patient or other person. Under the Preventing Harm Exception,[61] an Actor would not be Information Blocking if each of the following elements of this exception are met:

- **Reasonable Belief:** The Actor must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another person.[62]
- **Breadth of Practice:** The practice must be no broader than necessary to substantially reduce the particular risk of harm.[63]
- **Type of Risk:** The risk of harm must either:

  - be determined on an individualized basis in the exercise of the professional judgment of the provider with a current or prior clinician-patient relationship, or
  - arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.[64]

- **Type of Harm:** The specific types of harm that may be prevented under the Preventing Harm exception are aligned with the types of harm that must exist to deny access to PHI under the HIPAA Privacy Rule.[65] Depending on who is requesting EHI and the type of request, the type of harm must either be (1) to the life or physical safety of an individual or (2) substantial harm, which may include "substantial physical, emotional, or psychological harm."[66] The Preventing Harm exception sets out the following four categories and the type of harm that must be at issue:

  - Patient's legal representative is requesting to access, exchange or use the patient's EHI. The applicable type of harm, based on an individualized determination of risk of harm, is **substantial harm to the individual or another person**.
  - Patient or the patient's legal representative is requesting to access, exchange, or use the patient's EHI, and the EHI references another natural person. The applicable type of harm, based on an individualized determination of risk of harm, is **substantial harm to the other person**.
  - Patient is requesting to access, exchange, or use their EHI. The applicable type of harm is based either on an individualized determination of risk of harm or arising from data that is known or reasonably suspected to be corrupt due to technical failure, erroneous for another reason, or misidentified or mismatched, or **danger to the life or physical safety of the individual or another person**.
  - Patient's legal representative is requesting to access, exchange or use the patient's EHI. The applicable type of harm, arising from data that is known or reasonably suspected to be

misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason, is **danger to the life or physical safety of the individual or another person**.[67]

- **Patient right to request review of individualized determination of risk of harm.**[68]
- **Practice implemented based on an organizational policy or a determination specific to the facts and circumstances**.[69]

When an Actor seeks to rely on the Preventing Harm Exception, it is particularly important to pay attention to the type of harm they seek to avoid. The Preventing Harm exception aligns with the HIPAA Privacy Rule's standards for denying requests for PHI. ONC made it clear that a provider cannot cite the threat of non-physical harm to the patient or another individual as a reason to deny the patient access, exchange, or use of their own EHI.[70] There must be a danger to the life or physician safety of the patient.

The following is a chart to help visualize the application of these standards:

Who is requesting EHI?	Individual affected	Type of Harm	Information Blocking Regulation Reference	HIPAA Privacy Rule Standard
Patient's legal representative (including personal representative under HIPAA)	Patient or another person	Substantial harm to the patient or to another person	45 CFR 171.201(d)(1)	45 CFR 164.524(a)(3)(iii)
Patient or Patient's legal representative (including personal representative under HIPAA)	Another person	Substantial harm to such other person	45 CFR 171.201(d)(2)	45 CFR 164.524(a)(3)(ii)
Patient	Patient	Life or physical safety of the individual or another person	45 CFR 171.201(d)(3)	45 CFR 164.524(a)(3)(i)
Any "legally permissible" access, exchange or use of EHI not described in sections (d)(1)-(3)	N/A	Life or physical safety of the individual or another person	45 CFR 171.201(d)(4)	45 CFR 164.524(a)(3)(i)

COMPLIANCE TIP: Health care providers that have a practice of not sharing or delaying the release of provider notes and test results must reevaluate this practice in light of the Information Blocking rule. The Preventing Harm Exception may be available to justify this practice in limited circumstances, but providers need to carefully review the elements of this exception to determine if they are met. In particular, ONC has stated that the possibility of patient anxiety or other "psychological" harm will not justify the failure to release or delay the release of EHI. Actors should also consider a practice of developing an organizational policy or contemporaneously documenting the reason for denying or delaying access, use, or exchange of PHI. Although these situations are usually determined on a case-by-case basis with deference to the judgment of the clinician, the determination is subject to review if it is reviewable under HIPAA's Privacy Rule.

(ii) Privacy Exception

ONC created the Privacy Exception to allow an Actor to engage in practices that are reasonable and necessary to protect the privacy of an individual's EHI. To satisfy the Privacy Exception, an Actor's practice must meet at least one of the four sub-exceptions set out in the rule. The four sub-exceptions are:

- **Precondition not satisfied.** The Actor is required by a state or federal law to satisfy a precondition prior to providing access, exchange, or use of EHI, and that precondition has not been satisfied. An example of a precondition would be the execution of a patient consent or authorization. The Actor may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied under certain circumstances.[71]
- **Health IT Developer of Certified Health IT not covered by HIPAA.** If the Actor is a Health IT developer of Certified Health IT not covered by HIPAA, it will not be engaging in Information Blocking if the practice promotes the privacy interests of the individual and the practice is described in the Actor's organizational privacy policy that has been disclosed to the individual or entity that uses the Actor's health IT prior to their use.[72]
- **Denial of an individual's request for their EHI consistent with the HIPAA Privacy Rule.** An Actor that is a covered entity or business associate may deny an individual's request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) of the HIPAA Privacy Rule.[73]
- **Respecting an individual's request not to share information.** An Actor may deny the access, exchange, or use of EHI where an individual specifically requests that the Actor not do so. There must be no improper encouragement or inducement of the request by the Actor, the Actor must document the request within a reasonable time period, and the Actor's practice must be implemented in a consistent and nondiscriminatory manner. The Actor may only terminate the request as permitted by this sub-exception.[74]

COMPLIANCE TIP: The Privacy Exception is intended, in part, to align the Information Blocking rule with HIPAA, so an Actor should review its HIPAA compliance policy. Further, the fourth sub-exception could greatly aid an Actor seeking to protect against an Information Blocking complaint. To the extent an individual agrees to the practice, and that agreement is documented within a reasonable time period, this provision would defend against an Information Blocking claim. Finally, while the Rule does not require an Actor to violate the terms of Business Associate Agreement ("BAA") and the Rule was intended to operate in a manner consistent with the framework of the Privacy Rule, a BAA could constitute interference under the Rule if used in a discriminatory manner to forbid or limit access, use, or exchange of EHI that would otherwise be a permitted disclosure under the Privacy Rule. An Actor, therefore, should review its BAAs to determine whether there was any action taken by an Actor that was likely to interfere with the access, exchange, or use of EHI, and whether the Actor had the requisite intent.[75]

(iii) Security Exception

ONC recognized that the Information Blocking Rule may lead Actors to be reluctant to implement security measures or engage in activities reasonable and necessary to safeguard the confidentiality, integrity, and availability of EHI.[76] ONC noted that the discouragement of robust security measures would undermine the goals of the Information Blocking Rule.[77] To address that reluctance, ONC promulgated the Security Exception, which may apply to a practice where the Actor interferes with the access, exchange, or use of EHI to protect the security of EHI, provided the conditions of the exception are met.

For a practice to be eligible for the Security Exception, the Actor must demonstrate that it meets all of the following conditions:

- The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI;[78]
- The practice must be tailored to specific security risks being addressed;[79] and
- The practice must be implemented in a consistent and non-discriminatory manner.[80]

The Actor can meet these conditions either by (1) implementing a written organizational security policy,[81] or (2) making a determination based on particularized facts and circumstances that the practice was necessary to mitigate the security risk to EHI and there were no reasonable and appropriate alternatives to the practice less likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.[82]

If the practice is implementing an organizational security policy, four requirements must be met. First, the policy must be in writing.[83] Second, the policy must have been prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the Actor.[84] Third, the policy must align with one or more applicable consensus-based standards or best practice guidance.[85] Finally, the policy must provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.[86]

If the practice is based on particularized facts and circumstances, two requirements must be satisfied. First, there must have been a determination that the practice is necessary to mitigate the security risk to EHI.[87] Second, the Actor must have determined that there are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.[88]

COMPLIANCE TIP: This exception, as well as many other exceptions, will be available to an Actor who has developed organizational policies that contemplate use of these exceptions. Actors should review their organizational policies and procedures in light of each exception and either update or adopt appropriate policies and procedures.

(iv) Infeasibility Exception

ONC recognized that in certain circumstances there are legitimate practical challenges beyond an Actor's control that may limit its ability to comply with requests for access, exchange, or use of EHI.[89] These challenges include an Actor's lack of technical capabilities, legal rights, financial resources, or other means to provide a particular form of access, exchange, or use. In addition, the Actor may not be able to comply with the request without incurring costs or other burdens that are clearly unreasonable under the circumstances.[90] To alleviate this concern, ONC created the Infeasibility Exception, where a

practice is not Information Blocking if the Actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided one of the following conditions is met:

- **Uncontrollable events**: The Actor cannot fulfill the request for access, exchange, or use of EHI due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority that in fact negatively impacts the Actor's ability to fulfill the request.[91]
- **Segmentation**. The Actor cannot fulfill the request for access, exchange, or use of EHI because the Actor cannot unambiguously segment the requested EHI from EHI that cannot be made available due to an individual's preference or because the EHI cannot be made available by law, or may be withheld in accordance with the Preventing Harm exception.[92]
- **Third Party seeking modification use.** The request is to enable use of EHI in order to modify EHI provided that the request for such use is not from a health care provider requesting such use from an Actor that is its business associate.[93]
- **Manner exception exhausted.** The Actor is unable to fulfill a request for access, exchange or use of EHI under certain circumstances, and the Manner exception is satisfied.[94]

    - The Actor could not reach agreement with a requestor under the Manner exception or was technically unable to fulfill a request for EHI in the manner requested.
    - The Actor offered at least two alternative manners in accordance with the Manner exception.
    - The Actor does not provide the same access, exchange, or use of the requested EHI to a substantial number of individuals or entities that are similarly situated to the requestor.

        - The Actor may not discriminate based on whether the requestor is an individual, the size and type of health care provider, and whether the requestor is a competitor or would facilitate competition with the Actor.[95]

- **Infeasibility under the circumstances**. The Actor demonstrates, prior to responding to the request, through a contemporaneous written record or other documentation, its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstance.[96] The Actor may not consider whether the manner requested would have (1) facilitated competition with the Actor, or (2) prevented the Actor from charging a fee or resulted in a reduced fee.[97] Factors the Actor must consider are:

    - The type of EHI and the purposes for which it may be needed;
    - The cost to the Actor of complying with the request in the manner requested;
    - The financial and technical resources available to the Actor;
    - Whether the Actor's practice is non-discriminatory and the Actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
    - Whether the Actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged; and
    - Why the Actor was unable to provide access, exchange, or use of EHI consistent with the Content and Manner Exception.[98]

If the Actor does not fulfill a request for access, exchange, or use of EHI due to infeasibility, it must provide a written response to the requestor within 10 business days of receipt of the request with the reason why the request is infeasible.[99]

COMPLIANCE TIP: An Actor should maintain contemporaneous documentation when it is exercising this exception, or another exception where such documentation is relevant, because this documentation will be reviewed as part of an Information Blocking investigation by OIG and will likely help an Actor demonstrate compliance with the Information Blocking rule.

(v) Health IT Performance Exception

The fifth and final exception available where the Actor denies access, exchange, or use of EHI is the Health IT Performance Exception.[100] ONC observed that Actors need to engage in both planned and unplanned maintenance and improvement of health IT, and that these practices, if they fit the exception, would not constitute Information Blocking.[101] The Health IT Performance Exception is available to an Actor engaging in a practice intended to maintain or improve health IT performance if the practice satisfies one of four conditions: (1) maintenance and improvements to health IT; (2) assured level of performance; (3) practices that prevent harm, or (4) security related practices.[102]

- **Maintenance and improvements to health IT.** When an Actor implements a practice that makes health IT under that Actor's control temporarily unavailable, or temporarily degrades the performance of health IT, to perform maintenance or improvements to the health IT, the practice must be:
    - Implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;
    - Implemented in a consistent and non-discriminatory manner; and
    - If the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN, and it is:
        - Planned, then it must be consistent with existing service level agreements, or
        - Unplanned, then it must be consistent with existing service level agreements or agreed to by the individual or entity being supplied with the health IT.[103]
- **Assured level of performance.** An Actor may take action against a third-party application that is negatively impacting the health IT's performance, provided that the practice is:
    - For a period of time no longer than necessary to resolve any negative impacts;
    - Implemented in a consistent and non-discriminatory manner; and
    - Consistent with existing service level agreements, where applicable.[104]
- **Practices that prevent harm.** If the unavailability is in response to a risk of harm or the Actor must only comply with the Preventing Harm Exception.[105]
- **Security-related practices.** If the unavailability is in response to a security risk, the Actor must only comply with the Security Exception.[106]

(b) Subpart C - Exceptions That Involve Procedures for Fulfilling Requests to Access, Exchange, or Use Electronic Health Information

The next three Information Blocking exceptions are available to an Actor who is fulfilling requests to access, exchange, or use EHI, but not necessarily in the way requested. The three exceptions that fall into this category are (1) Manner, (2) Fees, and (3) Licensing. These exceptions are interrelated, and will likely be available to an Actor to use in a "layered" approach.

(i) Manner

The Manner exception permits an Actor to respond to a request to access, exchange, or use EHI in a manner that is different than what was requested, if the conditions of the Manner exception are satisfied.[107]

While an Actor must generally fulfill a request for EHI in the manner requested, the Manner condition permits the Actor to fulfill a request in an alternative manner when the Actor is (1) technically unable to fulfill the request in the manner requested; or (2) cannot reach agreeable terms with the requestor to fulfill the request in the manner requested.[108] If either of these conditions are satisfied, the Actor must fulfill the request in an alternative matter set forth in the exception.[109]

The first way that an Actor can fulfill a request in an alternative manner is if the Actor is technically unable to fulfill the request in the manner requested.[110] Under this exception, any fees charged by the Actor are not required to satisfy the Fees Exception or any license is not required to satisfy the Licensing Exception.[111] ONC emphasized that this means an Actor "cannot" fulfill the request due to a technical limitation.[112] According to ONC, this sets a "very high bar," and would not be satisfied if an Actor has a technical ability but chooses not to fulfill the request due to cost, burden, or similar reason.[113] If cost or burden is the true reason for denying a request, then the Actor should seek to comply with the Fees/Licensing, or Infeasibility Exceptions, respectively.[114]

The second way that an Actor can fulfill a request in an alternative manner is if the Actor cannot reach agreeable terms with the requestor.[115] ONC stated that if the Actor agrees to fulfill the request in any manner requested, then any fees or licenses associated with fulfilling the request will not be limited by the Fees or Licensing Exceptions.[116] However, if the Actor fulfills the request in an alternative manner, any fees or licensing must comply with the Fees or Licensing Exceptions.

If the Actor does not fulfill a request in any manner requested because it is technically unable or cannot reach agreeable terms with the requestor, then the Actor must fulfill the request in an alternative manner without unnecessary delay.[117] The Manner Exception creates an order of priority for determining an appropriate alternative manner of fulfillment.[118] First, the Actor must try to fulfill the request using ONC certified IT specified by the requestor.[119] Next, the Actor must use a content and transport standard specified by the requestor and published by the federal government or by a standards developing organization accredited by the American National Standards Institute (ANSI).[120] Third, the Actor can use an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.[121]If an Actor fulfills a request in one of these alternative manners, 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.[122]

(ii) Fees Exception

ONC generally views any fee that is likely to interfere with access, exchange, or use of EHI as Information Blocking, but recognized that a prohibition on fees would have unintended consequences on

innovation and competition.[123] ONC created the Fees Exception to allow an Actor to charge fees if the elements of the exception are satisfied. The Fees Exception, if satisfied, allows an Actor to charge fees that result in a reasonable profit margin.[124] It has three components. First, it sets forth the criteria for what a fee must be based on.[125] Second, it identifies the criteria that a fee must not be based on.[126] Finally, if applicable, it sets out conditions for a health IT developer subject to certain Conditions of Certification.[127]

As to the first component, a fee must be based on the following criteria:

- Objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests.
- Reasonably related to the Actor's cost of providing the type of access, exchange, or use of EHI to, or at the request of, the person or entity to whom the fee is charged.
- Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplies, or for whom the technology is supported.
- Based on costs not otherwise recovered for the same instance of service to a provider or third party.[128]

Under the second component, the fee must not be based on the following criteria:

- Whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the Actor;
- 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;
- Costs the Actor incurred due to the health IT being designed or implemented in a non-standard way, unless the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use the EHI;
- Costs associated with intangible assets other than the actual development or acquisition costs of such assets;
- Opportunity costs unrelated to the access, exchange, or use of EHI; or
- Any costs that led to the creation of intellectual property, if the Actor charged a royalty for that intellectual property under the Licensing Exception, and that royalty included the development costs for the creation of the intellectual property.[129]

In addition to these criteria that a fee must or must not include to satisfy this exception, the Fees Exception prohibits four types of fees:

- A fee prohibited under the HIPAA Privacy Rule for individuals requesting a copy of PHI;
- A fee based in any part on the electronic access[130] of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual;
- A fee to perform an export of EHI via the capability of health IT certified to the certification criterion for the purposes of switching health IT or to provide patients their EHI; and
- 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.[131]

Finally, the Fees Exception clarifies that a health IT developer of certified health IT subject to the API Conditions of Certification must comply with all requirements of such conditions of certifications for all practices and at all relevant times to qualify for the Fees Exception.[132]

(iii) Licensing Exception

Closely related to the Fees Exception, the Licensing Exception reflects ONC's general view that licensing interoperability elements for EHI to be accessed, exchanged, or used is Information Blocking, unless the Actor's practice satisfies the elements of the Licensing Exception.[133] Interoperability elements are "hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services" that may be necessary to access, exchange, or use EHI and are controlled by the Actor, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of electronic health information.[134] Under the Licensing Exception, the practice must meet three conditions: (1) negotiating a license timely, (2) providing the license under acceptable conditions, and (3) additional conditions relating to the provision of interoperability elements.[135]

The first condition under the licensing exception is that the Actor negotiates a license within the required time frame.[136] When an Actor receives a request to license an interoperability element, it must begin negotiations with the requestor within ten business days of receiving that request.[137] The Actor must then negotiate a license with the requestor within 30 business days from receipt of the request.[138]

Second, the license provided for the interoperability elements needed to access, exchange, or use electronic health information must meet five conditions.[139]

- Scope of rights. The license must provide all rights necessary to:
    - Enable the access, exchange, or use of electronic health information; and
    - Achieve the intended access, exchange, or use of electronic health information via the interoperability elements.[140]
- Reasonable royalty. If the Actor charges a royalty for the use of the interoperability elements, the royalty must be reasonable and comply with the following requirements:
    - The royalty must be nondiscriminatory, consistent with paragraph (b)(3) of the exception.
    - The royalty must be based solely on the independent value of the Actor's technology to the licensee's products, not on any strategic value stemming from the Actor's control over essential means of accessing, exchanging, or using electronic health information.
    - If the Actor has licensed the interoperability element through a standards developing organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on terms consistent with those in this exception, the Actor may charge a royalty that is consistent with such policies.
    - An Actor may not charge a royalty for intellectual property if the Actor recovered any development costs under the Fees Exception that led to the creation of the intellectual property.[141]
- Non-discriminatory terms. The terms (including royalty terms) on which the Actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements:
    - The terms must be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons and requests.
    - The terms must not be based in any part on -

- Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the Actor; or
- The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements.[142]

- Collateral terms. The Actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following -

  - Not compete with the Actor in any product, service, or market.
  - Deal exclusively with the Actor in any product, service, or market.
  - Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.
  - License, grant, assign, or transfer to the Actor any intellectual property of the licensee.
  - Pay a fee of any kind whatsoever, except a reasonable royalty permitted under the Licensing Exception, unless the practice meets the requirements of the Fees Exception.[143]

- Non-disclosure agreement. The Actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the Actor's trade secrets, provided -

  - The agreement states with particularity all information the Actor claims as trade secrets; and
  - Such information meets the definition of a trade secret under applicable law.[144]

Finally, the Licensing Exception lists additional considerations an Actor must follow relating to the provision of interoperability elements.[145] The Actor cannot engage in any practice that has the purpose or effect of (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.

(c) Subpart D – TEFCA Manner Exception

The third, and newest, category of exception is the TEFCA Manner Exception that is available to Actors that participate in TEFCA. The Trusted Exchange Framework and Common Agreement is a nationally trusted exchange framework and common agreement developed by ONC, with input from various stakeholders to provide a common set of principles, terms and conditions to enable nationwide exchange of EHI.[146] Under this exception, an Actor's practice of limiting the manner in which it fulfills a request for access, exchange, or use of EHI to only TEFCA will not be considered Information Blocking if the parties satisfy four conditions.[147] First, the Actor and requestor are both part of TEFCA.[148] Second, the requestor is capable of access, exchange or use of the requested EHI from the Actor via TEFCA.[149] Third, the request is not via the API standards adopted by ONC or other standards approved by the Standards Version Advancement Process.[150] Finally, any fees charged by the Actor and licensing of interoperability elements satisfy the respective Information Blocking exceptions.[151]

6. Did the Actor meet the required standard of knowledge?

For a practice to be Information Blocking, the Actor must have acted with the required level of knowledge.[152] The Information Blocking rule establishes different knowledge standard depending on the type of Actor involved. A Health Care Provider must have known that a practice was unreasonable and was likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI. A Health IT Developer of Certified Health IT, Health Information Exchange, or Health Information Network is held to the higher standard of knowledge that it must have known or should have known that a practice was likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

7. Actor has the Burden of Proof to show an Exception Applies

An Actor has the burden of proof to demonstrate that its practice is permitted by an Information Blocking exception.[153] ONC has commented that this allocation of proof is a substantive condition of the exception.[154] In ONC's view, the Actor is in the best position to demonstrate its compliance and to provide the detailed evidence in support. Such evidence may include written policies and procedures developed by the Actor. Even if a practice fails to satisfy an exception, an Actor can still rely on this evidence in an investigation to demonstrate that the practice did not rise to the level of interference or that the Actor lacked the requisite intent.[155]

II. Additional Information Blocking Considerations

A. Enforcement and Penalties

The Cures Act authorized OIG to investigate claims of Information Blocking and authorized the Secretary of HHS to impose Civil Monetary Penalties against certain individuals and entities that the OIG determines to have engaged in Information Blocking.[156] The Cures Act also directed the National Coordinator to implement a standardized process for the public to report claims of Information Blocking.[157] This complaint process is required to collect certain information, such as the originating institution, location, type of transaction, and related information.[158] By statute, any information received in connection with an Information Blocking complaint is exempt from public disclosure except as may be necessary to carry out the purpose of that section.[159] ONC has stated in commentary that it does not intend to make complaints publicly available.[160] ONC has developed a website allowing for public submission of Information Blocking complaints.[161]

1. Civil Money Penalties (Health IT Developers, HIE, HIN)

On July 3, 2023, OIG published its final rule authorizing civil money penalties (CMP) for Information Blocking ("CMP Final Rule").[162] Effective September 1, 2023, the CMP Final Rule gave OIG authority to investigate claims of Information Blocking and assess CMPs against three types of Actors subject to the Information Blocking Rule: (1) health IT developers of certified health IT, (2) health information networks, and (3) health information exchanges. OIG can impose a CMP of up to $1 million per violation.

Under the Cares Act, OIG may impose a penalty of not more than $1 million per violation of the CMP. The amount of the penalty imposed will depend on OIG's evaluation of two sets of factors: (1) those specific to the Information Blocking CMP in the Cares Act and (2) the general factors found in the Civil Monetary Penalties Law (CMPL). The CMPL contains a list of general factors that are applicable to all CMPs,[163] and the existing CMP regulatory framework sets forth aggravating and mitigating factors that the OIG will consider when considering a CMP.[164] These factors include the nature and circumstances of the violation, the degree of culpability, history of prior offenses, and other wrongful

conduct.[165] The CMP Final Rule sets forth additional factors that the OIG must consider when imposing a CMP specific to Information Blocking. These factors include the nature and extent of the Information Blocking and the harm resulting from such Information Blocking, including the number of patients affected, the number of providers affected, and the number of days that the Information Blocking persisted.[166] In its commentary to the CMP Final Rule, OIG listed its five enforcement priorities of the Information Blocking CMP.[167] OIG will focus specifically on Information Blocking conduct that: (1) resulted in, is causing, or had the potential to cause patient harm; (2) significantly impacted a provider's ability to care for patients; (3) was of long duration; (4) caused financial loss to federal healthcare programs or other government or private entities, and (5) was performed with actual knowledge.[168]

2. Appropriate Disincentives (Health Care Providers)

Under the Cures Act, OIG shall refer any health care provider that OIG has determined to engage in Information Blocking to the "appropriate agency" to be subject to "appropriate disincentives" using authorities under applicable federal law, as set forth in future rulemaking.[169]

On July 1, 2024, CMS and ONC published a final rule that sets forth the disincentives that an appropriate agency may impose on a health care provider that OIG determines has committed Information Blocking ("Disincentive Final Rule").[170] A "disincentive" is defined by the Disincentive Final Rule as a condition imposed on the health care provider for the purpose of deterring Information Blocking practices.[171] Not all health care providers as defined in 45 CFR 171.102 are subject to disincentives, but only those health care providers that are also Medicare-enrolled providers or suppliers. An "appropriate agency" to receive referrals from OIG and impose disincentives is defined by the Disincentive Final Rule as a "government agency that has established disincentives for health care providers."[172]

CMS is the "appropriate agency" to impose disincentives because "established disincentives" are available under three existing programs created by applicable federal law: (1) the Medicare Promoting Interoperability Program, (2) the Merit-based Incentive Payment System (MIPS), and (3) the Medicare Shared Savings Program. Thus, where OIG determines a health care provider has engaged in Information Blocking, it will refer the provider to CMS to impose an applicable disincentive.[173] CMS is required to send notice of disincentive to the health care provider with specific information such as a description of the practice forming the basis of the OIG's determination, the basis for the application of the disincentive, and the effect of the disincentive.[174]

The disincentive imposed on the health care provider is distinct under each program. Where a disincentive is imposed under the Medicare Promoting Interoperability Program, an eligible hospital or critical access hospital will not meet the definition of a meaningful electronic health record user in an EHR reporting period that OIG makes its referral.[175] As a result, an eligible hospital subject to this disincentive will not be able to earn the three quarters of the annual market basket increase associated with qualifying as a meaningful EHR user, and the critical access hospital subject to this disincentive would have its payment reduced to 100 percent of reasonable costs, from the 101 percent of reasonable costs it might have otherwise earned in an applicable year. Where the disincentive is imposed under the Merit-based Incentive Payment System (MIPS), eligible clinicians would not be considered a meaningful EHR user for MIPS, as that term is defined in federal regulations.[176] The consequence would be that the MIPS eligible clinician, if required to report on the Promoting Interoperability performance category of MIPS, would not earn a score in the performance category, which typically accounts for a quarter of the total final composite performance score. Finally, where the disincentive is imposed under the Medicare Shared Savings Program, an Accountable Care Organization (ACO), ACO participants, and ACO providers and suppliers would be removed from or denied approval to participate in the Medicare Shared Savings Program for at least one year.[177]

3. Public Posting

The Disincentive Final Rule also finalized ONC's proposal to post on its public website information about Actors who have been determined by OIG to have committed Information Blocking.[178] For health care providers who have been subject to a disincentive for Information Blocking, ONC will post the health care provider's (1) name, (2) business address, (3) the "practice" that was found to be Information Blocking, including when the "practice" occurred, (4) the disincentive, and (5) additional information about the determination that is publicly available from HHS.[179] ONC will post similar information for an HIE/HIN or Health IT Developer of Certified Health IT that the OIG has determined to have committed Information Blocking.[180] In both situations, this information will not be posted until the disincentive or CMP is finalized, including any applicable administrative appeals process.[181]

B. Relationship to State Law, HIPAA, and other Privacy Laws

The Information Blocking Rule enters an already crowded arena of patient privacy and health information laws at both the federal and state level. ONC drafted the Information Blocking Rule in communication with OCR so that the provisions of Information Blocking align with HIPAA. It is important to remember that HIPAA gives permission to share PHI under appropriate circumstances, while the Information Blocking Rule mandates access, use, or exchange of EHI, unless the rule does not apply or there is an applicable exception. For example, in the Preventing Harm Exception, ONC aligned the exception's standard of harm with the Privacy Rule's standard of harm. ONC also aligned the Privacy Rule with the provisions of the Privacy Exception. As to other federal and state laws, the Information Blocking Rule excludes from the definition of Information Blocking any practice where access, exchange, or use of EHI is "required by law."

III. Practical Operational and Compliance Tips

The Information Blocking Rule represents a paradigm shift in a health care provider's practices and attitudes towards sharing EHI. This paradigm shift requires not only a change in health care providers' attitudes, but also the adoption of new practices and procedures to comply with the Rule. The following are some operational and compliance suggestions to consider when adapting to the new world of Information Blocking.

a. **Develop Written Information Blocking Policy and Procedures.** A written Information Blocking policy and procedure can help identify where and how an organization might rely on exceptions to the Information Blocking Rule, respond to requests for EHI, develop internal audit practices, and address potential Information Blocking Rule complaints and investigations. A written policy and procedure will also assist in integrating the various stakeholders within the organization and allow the organization to assign responsibilities, coordinate responses, and document compliance efforts. Finally, several Information Blocking exceptions can be satisfied in part with a written organizational policy rather than invoking an exception on a case-by-case basis.
b. **Inventory current health IT capabilities.** Several Information Blocking exceptions, such as the Infeasibility, Content and Manner, Fees, and Licensing Exceptions are interrelated and depend on an understanding of the current and future health IT capabilities of the organization. Taking inventory of current health IT capabilities, and the organization's financial and technological capabilities will allow it to provide a quicker, more consistent response to requests for EHI. The organization will be able to better evaluate whether an exception to Information Blocking applies and how best to respond to a request for EHI.

c. **Developing Timely Response to Requests for EHI**. The Information Blocking Rule requires an Actor to timely assert an exception in response to a request to access, use or exchange EHI. For example, where an Actor wants to claim the Infeasibility Exception, it must respond to the request within 10 business days of receiving the request. Similarly, the Licensing Exception imposes a timeframe for negotiating a license with the requestor. Anticipating these requests for EHI and developing prepared responses will allow Actors to respond timely to these requests.

d. **Evaluate patient portal access to EHI**. To the extent that an organization offers patient portal access to EHI, the Information Blocking rule prioritizes a patient's access to their EHI. Actors should evaluate the types of EHI shared and the manner it is shared via a patient portal.

e. **Educate workforce on Information Blocking Rule Compliance.** Compliance with the Information Blocking Rule, like other regulatory schemes such as HIPAA, require workforce education and a change in organizational mindset. The Information Blocking Rule affects providers who write and enter notes into an EMR, HIM departments, compliance, legal, IT, and executive leadership. Every part of the organization that might have a role in decisions about the use, access, and exchange of EHI must be educated about the scope of the Information Blocking rule and trained in compliance. Like other health care regulations, Information Blocking introduces new requirements and standards to follow, and so requires organizational changes in mindset and culture. Where requests for use, access, and exchange of EHI would have been resisted, Information Blocking will force health care providers to shift to a posture of sharing and providing access, unless an exception applies.

f. **Evaluate Electronic Health Record Default Settings.** Actors using an EHR should consult with their EMR vendors to determine the capabilities of their EHR to comply with the Information Blocking Rule and any technical limitations or settings that may need to be adjusted. For example, an EMR may have default settings to sharing of physician notes or laboratory orders that may need to be enhanced or optimized to best comply with Information Blocking requirements.

g. **Review Contract Language.** Under the Information Blocking Rule, burdensome contractual terms, including BAAs, may constitute Information Blocking. Actors might consider reviewing contract language in the IT space as it relates to fees, licensing, and other terms that relate to use, access, or exchange of EHI for possible claims of interference.

h. **Monitor ONC for ongoing guidance and FAQs, and OIG for proposed rules**. ONC routinely provides sub-regulatory guidance in the form of FAQs posted on its website, among other written statements that provide guidance to understanding its interpretation of the Information Blocking Rule. However, Actors should exercise caution because this guidance is sub-regulatory, and other federal agencies like OIG might take the position it is not bound by such guidance. Also, there is still future rulemaking for penalties and disincentives by federal agencies.

i. **Coordinating with HIM.** To the extent an Actor has an HIM department that has historically handled responses to requests for EHI, it will want to coordinate those efforts with the various departments addressing Information Blocking requests and complaints. Actors will want to consider the role of HIM in Information Blocking compliance.

j. **EHR Donation Models.** Health care providers who donate their EHRs to other individuals or entities for use also likely meet the definition of a health IT developer of certified health IT under the Information Blocking rule, and would be required to satisfy the Information Blocking rule in that role as well.

k. **Document, Document, Document.** Several Information Blocking exceptions require the Actor to articulate contemporaneous reasons to support its reliance on that exception. For

example, the Preventing Harm exception requires in many circumstances an individualized assessment of the patient's request. Also, if the Actor seeks to claim infeasibility under the circumstances citing the Infeasibility Exception it must, prior to responding to the request, demonstrate the infeasibility through a contemporaneous written record or other documentation. In general, thoroughly documenting the use of Information Blocking exceptions will strengthen the Actor's defense against a possible complaint or investigation. The need to document is especially important because the Actor bears the burden of demonstrating that an Information Blocking exception applies to the challenged practice.

l. **Don't Play Favorites.** A recurring theme throughout the Information Blocking Exceptions it that an Actor implement practices in a consistent and non-discriminatory manner. Evaluate any current or proposed practices with an eye towards responding consistently to similarly situated requestors.

IV. Conclusion

Like HIPAA and PHI, the Information Blocking Rule has permanently changed the regulatory landscape for EHI. Health care providers must shift their mindset and adapt their current practices of handling EHI in response. The prohibition against Information Blocking is broad and captures many practices. The exceptions to Information Blocking are narrow, detailed and usually multifaceted. Actors who are subject to Information Blocking need to carefully understand these exceptions and prepare to rely on them if they intend to deny access, exchange, or use of EHI. For many organizations, significant time and effort was expended already to modify and adapt existing health IT in anticipation of the effective date of Information Blocking Rule. Now that Information Blocking is in effect, day-to-day compliance becomes all important. As of the date of this publication, it is unclear what enforcement actions the ONC, OIG, and other regulatory agencies will take against Information Blocking violations. However, proactive measures by an organization to comply with the letter and spirit of Information Blocking will ease the transition into this new world of health information sharing.

---

[1]21st Century Cures Act, Pub. L. No. 114-255, § 4004, 130 Stat. 1033, 1180 (2016).

[2] USC 300jj-52.

[3] ONC has since been dually titled as the Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (ASTP/ONC). See Federal Register: *Statement of Organization, Functions, and Delegations of Authority: Office of The National Coordinator for Health Information Technology*, 89 Fed Reg 60903 (July 29, 2024). For purposes of this white paper, all references will be to ONC.

[4]Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program*, 84 Fed Reg 7424 (March 4, 2019).

[5]Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program*, 85 Fed Reg 25642 (May 1, 2020). The regulations implementing Information Blocking are found at Part 171: 45 CFR 171.100-171.303. In addition to the Final Rule for Information Blocking, ONC simultaneously published provisions for Part 170 related to Conditions and Maintenance of Certification requirements for health IT developers. These portions of the Final Rule are outside the scope of this white paper.

[6]Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, *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 (November 4, 2020). In addition to extending the compliance date, ONC also extended other compliance dates associated with the Rule, for example, the expansion of the definition of EHI was extended to October 6, 2022.

[7]Office of Inspector General, Department of Health and Human Services, *Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules*, 88 Fed Reg 42820 (July 3, 2023); codified at 42 CFR Part 3.

[8]Centers for Medicare & Medicaid Services, Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, *21st Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking*, 88 Fed Reg 74947 (November 1, 2023).
[9]Centers for Medicare & Medicaid Services, Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, *21st Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking*, 89 Fed Reg 54662 (July 1, 2024).
[10]*Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing*, 89 Fed Reg 1192 (January 9, 2024).
[11]"Practice" is defined broadly by the Rule simply as "an act or omission by an actor." 45 CFR 171.102 (2024).
[12]As described more fully below, an Actor is a (1) health care provider, (2) health IT developer of certified health IT, (3) health information network, or (4) health information exchange. 45 CFR 171.102.
[13]"Access" is "the ability or means necessary to make electronic health information available for exchange or use." 45 CFR 171.102.
[14]"Exchange" is "the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks." 45 CFR 171.102.
[15]"Use" is "the ability for electronic health information, once accessed or exchanged, to be understood and acted upon." 42 CFR 171.102.
[16]45 CFR 171.103(a) (2024).
[17]45 CFR 171.101(2024). The statute uses the undefined phrases "health information technology developer, exchange, or network," and a "health care provider" so the Final Rule provided a more detailed definition of these types of actors.
[18]45 CFR 171.102(2024).
[19]The statutory definition, in full, states:

> "…hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center (as defined in section 300x–2(b)(1) of this title), renal dialysis facility, blood center, ambulatory surgical center described in section 1395l(i) of this title,[1] emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician (as defined in section 1395x(r) of this title), a practitioner (as described in section 1395u(b)(18)(C) of this title), a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe (as defined in the Indian Self-Determination and Education Assistance Act [25 U.S.C. 5301 et seq.]), tribal organization, or urban Indian organization (as defined in section 1603 of title 25), a rural health clinic, a covered entity under section 256b of this title, an ambulatory surgical center described in section 1395l(i) of this title,[1] a therapist (as defined in section 1395w–4(k)(3)(B)(iii) of this title), and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary." [42 USC 300jj].

[20]45 CFR 171.102 (2024).
[21]See 42 USC 300jj(5) where "health information technology" is defined as "hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information."
[22]45 CFR 171.102(2024).
[23]*Id*. ONC added this definition in the HTI-1 Final Rule to clarify what constitutes offering health IT.
[24] 45 CFR 171.102 (1), (2), and (3) (2024).
[25]85 Fed Reg 25799 (May 1, 2020).
[26]45 CFR 171.102 (2024).
[27]*Id*.
[28]*Id*. (defining EHI as "electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103" except EHI excludes 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.).
[29]See 45 CFR 160.103 (2024). Electronic protected health information is PHI that is transmitted or maintained in electronic media. *Id.* PHI, in turn, is defined as individually identified health information. *Id*. Individually identifiable health information is health information created or received by a health care provider, health plan,

employer, or health care clearinghouse that (1) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and either identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. *Id*.

[30]See 45 CFR 164.501 (2013).

[31]*Id*. The Rule did not implement the full definition of EHI on October 6, 2022. Prior to October 6, 2022, the information subject to Information Blocking is defined by the United States Code Data for Interoperability ("USCDI") standard. Because the definition of EHI is broad, ONC did not immediately apply the full definition of EHI to allow time for actors to adjust their operations to meet this new definition. Rather, the Rule adopted the standards of USCDI to define the scope of data elements that are subject to Information Blocking. Before October 6, 2022, EHI for the purposes of the Information Blocking definition was limited to the EHI identified by the data elements represented in the USCDI standard. On and after October 6, 2022, an actor must respond to a request to access, exchange, or use EHI under the full definition of EHI.

[32]45 CFR 171.103(a) (2024).

[33]45 CFR 171.102 (2024).

[34]85 Fed Reg 25808 (May 1, 2020).

[35]85 Fed Reg 25811 (May 1, 2020).

[36]85 Fed Reg 25812 (May 1, 2020).

[37]*Id*.

[38]*Id*.

[39]Fast Healthcare Interoperability Resources standard "defines how information can be exchanged between different computer systems regardless of how it is stored in those systems. The Office of the National Coordinator for Health Information Technology, *What Is FHIR?,* https://www.healthit.gov/sites/default/files/2019-08/ONCFHIRFSWhatIsFHIR.pdf (last accessed December 31, 2024).

[40]85 Fed Reg 25813 (May 1, 2020).

[41]*Id*.

[42]*Id*.

[43]85 Fed Reg 25817(May 1, 2020).

[44]85 Fed Reg 25818 (May 1, 2020).

[45]45 CFR 171.103(a) (2024).

[46]See 85 Fed Reg 25794 (May 1, 2020)..

[47]*Id*.

[48]45 CFR 171.200-205 (2020); 45 CFR 171.300-303 (2020).

[49]85 Fed Reg 25820 (May 1, 2020).

[50]45 CFR 171.300 (2020). In its commentary, ONC asserted that "failure to meet an exception does not necessarily mean a practice meets the definition of Information Blocking. If subject to an investigation, each practice that implicates the Information Blocking provision and does not meet an exception would be analyzed on a case-by-case basis to evaluate, for example, whether it rises to the level of an interference, and whether the actor acted with the requisite intent." 85 Fed Reg 25819 (May 1, 2020).

[51]45 CFR 171 Subpart B.

[52]45 CFR 171.201 (2020).

[53]45 CFR 171.202 (2024).

[54]45 CFR 171.203 (2020).

[55]45 CFR 171.204 (2024).

[56]45 CFR 171.205 (2020).

[57]45 CFR 171Subpart C.

[58]45 CFR 171.301 (2024).

[59]45 CFR 171.302 (2020).

[60]45 CFR 171.303 (2020). In the event of an investigation, ONC stated in its commentary that an Actor must demonstrate that the exception is applicable and that all the conditions of the relevant exception were met at all relevant times. 85 Fed Reg 24819 (May 1, 2020).

[61]45 CFR 171.201 (2020).

[62]45 CFR 171.201(a) (2020).

[63]45 CFR 171.201(b) (2020).

[64]45 CFR 171.201(c) (2020).

[65]45 CFR 164.524 (2017).

[66]See, for example, HIPAA Privacy Rule preamble at 65 FR 82556 (December 28, 2000).
[67]45 CFR 171.201(d) (2020).
[68]45 CFR 171.201(e) (2020).
[69]45 CFR 171.201(f) (2020).
[70]See discussion at 85 Fed Reg 25824(May 1, 2020).
[71]45 CFR 171.202(b) (2024).
[72]45 CFR 171.202(c) (2024).
[73]45 CFR 171.202(d) (2024).
[74]45 CFR 171.202(e) (2024).
[75]See discussion at 85 Fed Reg 25812 (May 1, 2020).
[76]85 Fed Reg 25859 (May 1, 2020).
[77]*Id*.
[78]45 CFR 171.203(a) (2020).
[79]45 CFR 171.203(b) (2020).
[80]45 CFR 171.203(c) (2020).
[81]45 CFR 171.203(d) (2020).
[82]45 CFR 171.203(e) (2020).
[83]45 CFR 171.203(d)(1) (2020).
[84]45 CFR 171.203(d)(2) (2020).
[85]45 CFR 171.203(d)(3) (2020).
[86]45 CFR 171.203(d)(4) (2020).
[87]45 CFR 171.203(e)(1) (2020).
[88]45 CFR 171.203(e)(2) (2020).
[89]85 FR 25865 (May 1, 2020).
[90]85 FR 25865-25866 (May 1, 2020).
[91]45 CFR 171.204(a)(1) (2024).
[92]45 CFR 171.204(a)(2) (2024).
[93]45 CFR 171.204(a)(3) (2024).
[94]45 CFR 171.204(a)(4) (2024).
[95]45 CFR 171.204(a)(4)(iv) (2024).
[96]45 CFR 171.204(a)(5)(i) (2024).
[97]45 CFR 171.204(a)(5)(ii) (2024).
[98]45 CFR 171.204(a)(5)(i)(A)-(F) (2024).
[99]45 CFR 171.204(b) (2024).
[100]45 CFR 171.205 (2020).
[101]85 Fed Reg 25870 (May 1, 2020).
[102]45 CFR 171.205 (2020).
[103]45 CFR 171.205(a) (2020).
[104]45 CFR 171.205(b) (2020).
[105]45 CFR 171.205(c) (2020).
[106]45 CFR 171.205(d) (2020).
[107]This exception originally was called the "Content and Manner" exception, but OCR removed the "Content" component because it is no longer necessary and revised this exception accordingly in the HTI-1 Final Rule. As discussed previously, until October 6, 2022, an actor was required to respond to a request for EHI with only the EHI identified by the data elements represented in the USCDI standard. After October 6, 2022, an actor must respond to a request using the full definition EHI found at § 171.102. Under the Content component of the Content and Manner exception prior to October 6, 2022, an actor was permitted to respond to a request with a narrower scope of EHI.
[108]45 CFR 171.301(a)(1) (2024). Technically unable means cannot fulfill a request due to a technical limitation.
[109]45 CFR 171.301(b) (2024).
[110]45 CFR 171.301(a) (2024).
[111]45 CFR 171.301(a)(2)(i), (ii) (2024).
[112]85 Fed Reg 25877 (May 1, 2020).
[113]*Id*.
[114]*Id*.
[115]45 CFR 171.301(a) (2024).

[116]*Id*.
[117]45 CFR 171.301(b)(1) (2024).
[118]*Id*.
[119]45 CFR 171.301(b)(1)(i) (2024).
[120]45 CFR 171.301(b)(1)(ii) (2024).
[121]45 CFR 171.301(b)(1)(iii) (2024).
[122]45 CFR 171.301(b)(2), (3) (2024).
[123]85 Fed Reg 25879 (May 1, 2020).
[124]45 CFR 171.302 (2020).
[125]45 CFR 171.302(a) (2020).
[126]45 CFR 171.302(b) (2020).
[127]45 CFR 171.302(c) (2020).
[128]45 CFR 171.302(a)(1) (2020).
[129]45 CFR 171.302(a)(2) (2020).
[130]Electronic access is defined as "an internet-based method that makes electronic health information available at the time the electronic health information is requested and where no manual effort is required to fulfill the request." 45 CFR 171.302(d) (2020).
[131]45 CFR 171.302(b) (2020).
[132]45 CFR 171.302(c) (2020).
[133]45 CFR 171.303 (2020).
[134]45 CFR 171.102 (2024).
[135]45 CFR 171.303(a), (b), (c) (2020).
[136]45 CFR 171.303(a) (2020).
[137]45 CFR 171.303(a)(1) (2020).
[138]45 CFR 171.303(a)(2) (2020).
[139]45 CFR 171.303(b) (2020).
[140]45 CFR 171.303(b)(1) (2020).
[141]45 CFR 171.303(b)(2) (2020).
[142]45 CFR 171.303(b)(3) (2020).
[143]45 CFR 171.303(b)(4) (2020).
[144]45 CFR 171.303(b)(5) (2020).
[145]45 CFR 171.303(c) (2020).
[146]TEFCA arose out of Section 4003 of the Cures Act. ONC established rules in 42 CFR part 172 that codified several aspects of TEFCA. See *Health Data, Technology, and Interoperability: Trusted Exchange Framework and Common Agreement*, 89 Fed Reg 101772 (Dec. 16, 2024) ("HTI-2").
[147]45 CFR 171.403(2024).
[148]45 CFR 171.403(a)(2024).
[149]45 CFR 171.403(b)(2024).
[150]45 CFR 171.403(c)(2024).
[151]45 CFR 171.403(d)(2024). HTI-2 also amended the Information Blocking Rule by including definitions related to the TEFCA Manner Exception. See 45 CFR 171.401 (2024).
[152]42 USC 300jj-52(a)(1)(B); 45 CFR 171.103 (2024).
[153]See 85 Fed Reg 25819 (May 1, 2020) ("We proposed that, in the event of an investigation of Information Blocking complaint, an actor must 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.").
[154]*Id.*
[155]85 Fed Reg 25820 (May 1, 2020).
[156]42 USC 300jj-52(b).
[157]PL 114-255 § 3022(d)(3)(A), 130 Stat. 1033.
[158]PL 114-255 § 3022(d)(3)(B), 130 Stat. 1033.
[159]PL 114-255 § 3022(d)(2), 130 Stat. 1033.
[160]85 Fed Reg 25900 (May 1, 2020). However, ONC warned Health IT Developers of Certified Health IT that it publishes in the Certified Health IT Product List (CHPL) information about non-conformities with the Information Blocking condition of certification requirements. *Id*.
[161]See *Welcome to the Health IT Feedback and Inquiry Portal*, http://www.healthIT.gov/healthITcomplaints (last accessed December 31, 2024).

[162]*Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules*, 88 Fed Reg 42820 (July 3, 2023); 42 CFR 1003.100-1003.1600 (2023). The OIG published a proposed rule on April 24, 2020, which would add a new Subpart N to the CMP regulations giving OIG authority to impose CMPs for Information Blocking committed by a Health IT Developer, or HIE/HIM. See 80 Fed Reg 22979 (April 24, 2020).
[163]42 USC 1320a-7a.
[164]42 CFR 1003.140 (2023).
[165]*Id*.
[166]42 CFR 1003.1420 (2023).
[167]88 Fed Reg 42822-42823 (July 3, 2023).
[168]88 Fed Reg 42822 (July 3, 2023).
[169]PL 114-255 § 3022(b)(2)(B), 130 Stat. 1033.
[170]*21st Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking*, 89 Fed Reg 54662 (July 1, 2024). CMS and ONC published the proposed final rule for disincentives on November 1, 2023 ("Disincentive Proposed Rule"). See *21st Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking*, 88 Fed Reg 74947 (November 1, 2023).
[171]45 CFR 171.102 (2024).
[172]*Id*.
[173]Similar to OIG's enforcement priorities with respect to the Information Blocking CMP, OIG states that it expects to prioritize, in its investigation of health care providers, cases (1) resulting in or causing patient harm, (2) significantly impacting a provider's ability to care for patients, (3) of long duration, and (3) causing financial loss to Federal health care programs, or other government or private entities. See 88 Fed Reg 74951 (November 1, 2023).
[174]45 CFR 171.1002 (2024).
[175]45 CFR 171.1001(a)(1) (2024).
[176]45 CFR 171.1001(a)(2) (2024).
[177]45 CFR 171.1001(a)(3) (2024).
[178]45 CFR 171.1101 (2024).
[179]45 CFR 171.1101(a) (2024).
[180]45 CFR 171.1101(b) (2024).
[181]45 CFR 171.1101 (2024).