healthcurrent

Information Blocking FAQs:

What health care providers need to know about information blocking compliance

Last updated: September 7, 2020
Authors: Melissa Soliz (partner) and Caitlin Donovan (affiliate), Coppersmith Brockelman PLC
Key Legal Citations: 42 U.S.C. 300jj-52; 45 CFR Part 171; ONC Cures Act Final Rule (85 Fed. Reg. 25462)

The compliance deadline is November 2, 2020.

The Office of the National Coordinator for Health Information Technology (ONC) published the Information Blocking Final Rule on May 1, 2020. The Information Blocking Rule (45 C.F.R. Part 171) went into effect on June 30, 2020. The compliance deadline is November 2, 2020. The Information Blocking Rule implements a requirement of the 21st Century Cures Act, which penalizes health care providers, health information technology (IT) developers, health information networks (HINs) and health information exchanges (HIEs) that impermissibly interfere with the access, exchange or use of electronic health information (EHI).

Compliance with the Information Blocking Rule is forcing the health care industry to rethink how health information is shared electronically. This document pulls together the questions health care providers are asking about the Information Blocking Rule and provides the educational content providers need to know about information blocking compliance. However, the Information Blocking Rule is new and complex. Health care providers and other readers of these FAQs should seek the advice of legal counsel regarding how the Information Blocking Rule applies to their specific situation.

FAQ CATEGORIES

WHAT IS INFORMATION BLOCKING?

What are the legal requirements of an information blocking claim?

An information blocking claim must include all of the following elements:

- An actor regulated by the Information Blocking Rule;
- Electronic health information (EHI);
- A practice that is likely to interfere with the access, exchange, or use of EHI;
- Requisite intent by the actor;
- The practice is not required by law; and
- The practice is not covered by one or more of 8 regulatory exceptions. We refer to these exceptions as "safe harbors" for practices that would otherwise implicate the Information Blocking Rule.

We break down each of these legally required elements in these FAQs. This Section of the FAQs focuses on what it means for an actor to engage in a practice that is likely to interfere with the access, exchange or use of EHI.

What does it mean for a health care provider to engage in a "practice" that is "likely to interfere with" the "access, exchange or use" of EHI?

The Information Blocking Rule penalizes actors, including health care providers, that engage in "practices" that are "likely to interfere with" the "access, exchange or use" of EHI, so long as the actor acts with the requisite level of intent and the practice is not required by law or covered by one or more regulatory safe harbors.

An actor engages in a "practice" when the actor either affirmatively does something—an act—or does nothing—an omission. Thus, any action or inaction by an actor might implicate the Information Blocking Rule if it is "likely to interfere with" the "access, exchange or use" of EHI.

"Likely to interfere with" means that there is a reasonably foreseeable risk (even if the harm does not actually materialize) that the practice will prevent, materially discourage, or otherwise inhibit any of the following:

- The ability or means necessary to make EHI available for exchange or use (*i.e.*, accessed);
- The ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks (*i.e.*, exchanged); and/or
- The ability for EHI, once accessed or exchanged, to be understood and acted upon (*i.e.*, used).

What kinds of practices might give rise to an information blocking claim?

ONC provides many examples of actor practices that might implicate the Information Blocking Rule in the preambles to the Information Blocking Proposed Rule (84 Fed. Reg. 7424, 7518-7521) and Information Blocking Final Rule (85 Fed. Reg. 25642, 25805-25818). ONC gives the following illustrative examples of practices that health care providers might engage in that would implicate the Information Blocking Rule:

- "A health system's internal policies or procedures require staff to obtain an individual's written consent before sharing any of a patient's EHI with unaffiliated providers for treatment purposes even though obtaining an individual's consent is not required by state or federal law."
- "A health system incorrectly claims that the HIPAA Rules or other legal requirements preclude it from exchanging EHI with unaffiliated providers."
- "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."

- "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."
- "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."
- "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."
- "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 more costly 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."

Additionally, ONC generally regards practices that result in the denial of a patient's access rights, or that impose fees on a patient's access (including access by a personal representative or a designated third party, like a personal health record application developer) to be "highly" or "inherently" suspect.[1] Indeed, ONC emphasizes that practices that interfere with the exchange, access or use of EHI for the following purposes will almost always implicate the Information Blocking Rule and will be "inherently suspect":

- "Providing patients with access to their EHI and the ability to exchange and use it without special effort";
- "Ensuring that health care professionals, care givers, and other authorized persons have the EHI they need, when and where they need it, to make treatment decisions and effectively coordinate and manage patient care and can use the EHI they may receive from other sources";
- "Ensuring that payers and other entities that purchase health care services can obtain the information they need to effectively assess clinical value and promote transparency concerning the quality and costs of health care services";
- "Ensuring that health care providers can access, exchange, and use EHI for quality improvement and population health management activities"; and
- "Supporting access, exchange, and use of EHI for patient safety and public health purposes."[2]

May the terms of a health care provider's business associate agreement (BAA) implicate the prohibition against information blocking?

Yes. ONC emphasizes that "formal restrictions, such as contract or license terms, EHI sharing policies, organizational policies or procedures, or other instruments or documents that set forth requirements related to EHI or health IT,"[3] are one of the potential forms of information blocking the Information Blocking Rule seeks to address. Indeed, BAAs are intended to restrict how a business associate may use and disclose protected health information. But whether a BAA actually violates the Information Blocking Rule depends on its terms, and whether those terms fall within a regulatory safe harbor. For example, the ONC warns that when a BAA is "entered into by one or more actors that permits access, exchange, or use of EHI by certain health care providers for treatment" that BAA "should generally not prohibit or limit the access, exchange, or use of the EHI for treatment by other health care providers of a patient."[4]

Will giving patients information about third party application privacy practices constitute an interference with the patient's access, exchange or use of EHI?

No, so long as all the following requirements are met with respect to the information provided:

- The information focuses on current privacy and/or security risks posed by the third-party application;
- This information is factually accurate, unbiased, objective, and not unfair or deceptive; and
- The information is provided in a non-discriminatory manner. This means that "all third-party apps must be treated the same way in terms of whether or not information is provided to individuals about the privacy and security practices employed."[5]

ONC also emphasizes that: **"To be clear, an actor may not prevent an individual from deciding to provide its EHI to a technology developer or app despite any risks noted regarding the app itself or the third-party developer."**[6]

WHO IS REQUIRED TO COMPLY WITH THE INFORMATION BLOCKING RULE?

To whom does the Information Blocking Rule apply?

The Information Blocking Rule applies to three categories of actor:

- Health care providers (as defined in 42 U.S.C. § 300jj);
- Health IT developers of certified health IT (CHIT); and
- Health information networks (HINs) and health information exchanges (HIEs).

Are all health care providers subject to the Information Blocking Rule?

For purposes of the Information Blocking Rule, a health care provider is a:

- Hospital;
- Skilled nursing facility;
- Nursing facility;
- Home health entity (or other long-term care facility);
- Health care clinic;
- Community mental health center;
- Renal dialysis facility;
- Blood center;
- Ambulatory surgical center;
- Emergency medical services provider;
- Federally qualified health center (FQHC);
- Group practice;
- Pharmacist;
- Pharmacy;
- Laboratory;
- Physician;
- Practitioner;
- Provider operated by or under contract with the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization;
- Rural health clinic
- Covered entity under section 42 U.S.C. § 256b;
- Therapist; and
- Any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.

Please see ONC's Health Care Provider Definition and Cross-Reference Table for a breakdown of the specific health care providers that fall into these categories.

Can a health care provider be subject to the Information Blocking Rule as a HIE/HIN?

Yes. A HIE/HIN is a functionality defined as "an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information:

> (1) Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and
> (2) That is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164."[7]

Thus, a health care provider that operates a care coordination platform that enables unaffiliated health care providers to exchange electronic health information (EHI) for treatment, payment or limited health care operations purposes may also be a HIE/HIN with respect to the practices associated with the access, exchange or use of EHI in connection with that platform.

Can a health care provider be subject to the Information Blocking Rule as a health IT developer of CHIT?

Yes. A health IT developer of CHIT means "an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops **or offers health information technology** (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information

blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj11(c)(5) (ONC Health IT Certification Program)."[8]

Health care providers who self-develop their own CHIT are excluded from the definition. But if a health care provider either offers their self-developed CHIT, or offers CHIT developed by others, to other entities "on a commercial basis or otherwise" they may be a health IT developer of CHIT.[9]

However, ONC explains that the following activities of health care providers will not trigger this definition:

- Use of APIs;
- Patient portals; and
- Providing login credentials to licensed health care professionals who are in independent practice to use a hospitals EHR (for example) to furnish and document care to patients in the hospital. This includes clinician portals used for this purpose.

WHAT INFORMATION IS SUBJECT TO THE INFORMATION BLOCKING RULE?

Does the Information Blocking Rule apply to all of an individual's health information?

No. The Information Blocking Rule only applies to electronic health information (EHI). EHI is defined as electronic protected health information (ePHI) that is in a designated record set (as those terms are defined by HIPAA,[10] but regardless of whether the EHI is maintained by or for a HIPAA covered entity).[11] A designated record set held by a health care provider includes:

- Medical and billing records about individuals; and
- Other records used, in whole or in part, by or for a health care provider to make decisions about individuals, including if those records originate from a source other than the health care provider (such as another health care provider or a payer).

EHI does **not** include:

- Psychotherapy notes (as defined by HIPAA); or
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Additionally, the amount of EHI actors must be able to provide access to is limited until **May 2, 2022** to those data elements represented in version 1 (v1) of the United States Core Data for Interoperability (USCDI).

What does it mean for the EHI to be represented by the USCDI (v1) data elements?

The USCDI data elements are a standardized set of health data classes and data elements that are to be utilized during the initial implementation phase of the information blocking rule. A USCDI data element is the most granular level at which a piece of data is represented in the USCDI for exchange.

Importantly, health care providers are **not** required at this time to maintain EHI in the USCDI (v1) data format or provide access to it in this format. These data elements are simply used as reference points for the minimum amount of EHI that is subject to the Information Blocking Rule until May 2, 2022. For example, x-ray images are not included among the USCDI (v1) data elements. Thus, even though a patient's digital x-ray image of his or her broken limb might be part of a designated record set maintained by a health care provider, it is not subject to the Information Blocking Rule until May 2, 2022.

Does EHI include de-identified data?

No. De-identified data that meets the HIPAA standards for de-identification are not included within the definition of EHI and thus is not subject to the Information Blocking Rule.

Does EHI include financial and cost information?

It depends. EHI includes ePHI that is maintained as part of a designated record set. Patient billing records, which include financial and cost information, are by definition part of a patient's designated record set. Additionally, such information might be used to make decisions about individuals, such as whether to continue providing non-emergency medical services to a patient who does not pay his or her bill. However, financial/cost information is not included in the USCDI (v1) data elements.[12] This means that until May 2, 2022, such information is not subject to the Information Blocking Rule.

WHAT WILL ENFORCEMENT OF THE INFORMATION BLOCKING RULE LOOK LIKE?

Which regulatory body is in charge of enforcing the Information Blocking Rule?

ONC is responsible for creating and maintaining the information blocking reporting system. Complaints of information blocking may be submitted to ONC using ONC's online form. The Office of the Inspector General (OIG) for the U.S. Department of Health & Human Services (HHS) is responsible for investigating claims of information blocking against all actors.

What are the penalties for violating the Information Blocking Rule?

If the OIG concludes that an actor has violated the Information Blocking Rule, the OIG may impose a civil monetary penalty (CMP) of up to $1 million per violation against an actor that is a health IT developer of certified health information technology (CHIT) or health information network (HIN) / health information exchange (HIE).

OIG will refer health care providers to the appropriate agency to be subject to appropriate disincentives. For example, under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), Public Law 114-10, and its implementing regulations (81 Fed. Reg. 77008), health care providers are required to make attestations supporting the prevention of information blocking. OIG's determination that a health care provider who participates in Medicare has engaged in information blocking may be referred to CMS for appropriate disincentives under MACRA. OIG may also refer health care providers to the Office for Civil Rights (OCR), in the event the information blocking practice also constitutes a violation of HIPAA (such as a violation of an individual's HIPAA access rights).

When will the OIG start enforcing the Information Blocking Rule with CMPs?

The Information Blocking Rule went into effect on June 30, 2020. However, enforcement is delayed until at least November 2, 2020—the compliance date of the Information Blocking Rule. Enforcement may be further delayed depending on when the OIG finalizes its proposed rule on CMPs (see 85 Fed. Reg. 22979), and whether the OIG further delays the enforcement deadline in the CMP final rule. In the preamble to the CMP proposed rule, OIG states that: "Conduct that occurs before the effective date of our final rule will not be subject to information blocking CMPs."[13]

What does the OIG look for when evaluating corporate compliance programs?

The OIG has not yet issued guidance on how it will evaluate a health care provider's compliance with the Information Blocking Rule. However, in informal discussion groups and presentations, OIG representatives have stated that they anticipate enforcing the Information Blocking Rule similar to their enforcement of other health care laws, like the federal Anti-Kickback Statute (AKS).

When evaluating other health care compliance programs (such as AKS compliance), the OIG asks the following three fundamental questions:

- Is the compliance program well designed?
- Is the program being applied earnestly and in good faith? That is, is the program adequately resourced and empowered to function effectively?
- Does the compliance program work in practice?[14]

In answering these questions, the OIG will consider whether the compliance program incorporates the following 7 key program elements:

- Standards, policies, and procedures;

- Compliance program administration;
- Screening and evaluation of employees, physicians, vendors and other agents;
- Communication, education, and training on compliance issues, including a mechanism for evaluating employee understanding of compliance responsibilities;
- Monitoring, auditing, and internal reporting systems, including anonymous reporting;
- Discipline for non-compliance, including adherence to a non-retaliation policy for reporters; and
- Investigations and remedial measures.

For more information on how to structure an effective compliance program, please review the U.S. Department of Health and Human Services Office of Inspector General (OIG)'s Resource Guide and Compliance Guidance. We also offer some tips and suggestions for how to incorporate information blocking compliance into your existing compliance structure in the FAQ section on "How to implement compliance."

May individuals within an Actor's organization be held liable for information blocking?

Yes. The OIG has authority to investigate and impose penalties on an "individual or entity" that is an actor and whom the OIG determines to have committed information blocking.[15]

Are Information Blocking Complaints to the ONC discoverable under the Freedom of Information Act (FOIA)?

No. Information blocking complaints are confidential and not publicly available.

WHAT PRACTICES DO NOT CONSTITUTE INFORMATION BLOCKING?

Does the Information Blocking Rule require health care providers to share electronic health information (EHI) with anyone who requests it, even if the requirements of other state and federal laws have not been met?

No. The Information Blocking Rule does not preempt or supersede other federal, state or local laws, like HIPAA or 42 C.F.R. Part 2 (the federal Confidentiality of Substance Use Disorder Treatment regulations). Health care providers must comply with both the Information Blocking Rule and other federal, state or local health information privacy laws that apply to them. Indeed, it is **not** information blocking if the practice that interferes with the access, exchange or use of EHI is:

- Required by law;
- Covered by a regulatory safe harbor, such as the privacy safe harbor; or
- Done by the actor without the required level of intent.

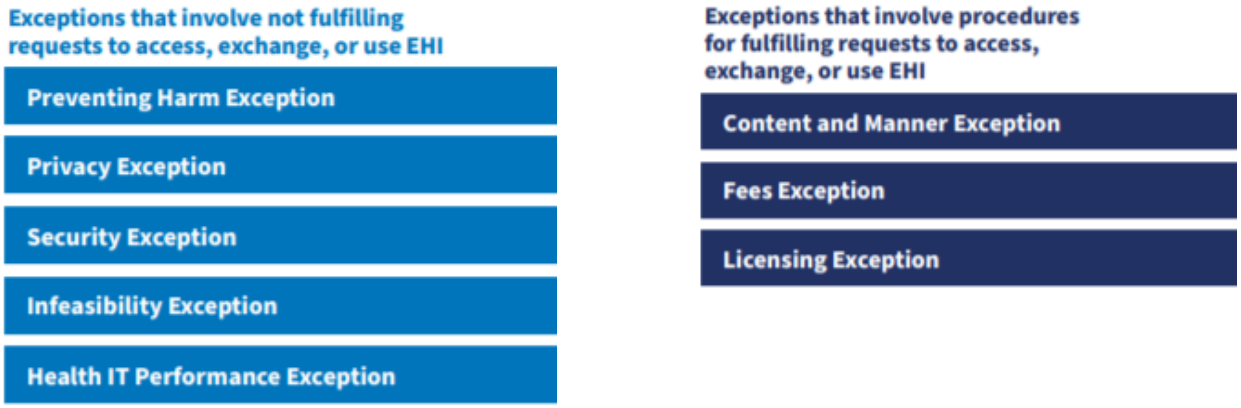
What does "required by law" mean?

Required by law means that the interference is "explicitly required by State or Federal law."[16] State and federal laws include statutes, regulations, court orders, binding administrative decisions or settlements (including the Federal Trade Commission (FTC) or Equal Employment Opportunity Commission (EEOC)), as well as tribal law (as applicable). ONC does not consider state or federal privacy laws that require patient authorization or consent for the disclosure of EHI, for example, to constitute an interference "required by law." Rather, ONC categorizes such interferences as practices "engaged in pursuant to a privacy law, but which are not 'required by law.'"[17] In such cases, an actor must look to a regulatory safe harbor.

What are the regulatory exceptions (safe harbors)?

Practices that are covered by a regulatory safe harbor will not constitute information blocking. There are 8 regulatory safe harbors that can be divided into two categories:

- Practices that involve partially or entirely denying requests to access, exchange or use EHI; and
- Practices that involve procedures for fulling the requests.



ONC, Cures Act Final Rule: Information Blocking Exceptions.

For more information about the exceptions please see the FAQ section on "What is the intent and purpose of the regulatory safe harbors."

What level of intent is required to constitute a violation of the Information Blocking Rule?

It depends on the type of actor. Health care providers who engage in information blocking practices must know that the practice is unreasonable and likely to interfere with the access, exchange or use of EHI. By contrast, health IT developers of CHIT and HIE/HINs need only know or should have known that the practice was likely to interfere with access, exchange or use of EHI. OIG has stated that it will not bring enforcement actions against actors who make "innocent mistakes."[18]

Who bears the burden of proving that the practice does or does not constitute information blocking?

The OIG will determine whether an actor's practice implicates the Information Blocking Rule and whether an actor acted with the requisite level of intent. However, actors bear the burden of proving that the practice at issue qualifies for a regulatory safe harbor.

WHAT IS THE INTENT AND PURPOSE OF THE REGULATORY SAFE HARBORS?

The regulatory safe harbors are complex, and their application is highly fact specific. Thus, this section of the FAQs only provides a high-level summary of the intent and purpose of the regulatory safe harbors.

What is the general intent and purpose of the regulatory safe harbors?

Congress gave the Secretary of Health and Human Services (HHS) the authority to identify reasonable and necessary activities that do **not** constitute information blocking. HHS delegated this task to ONC. ONC has created 8 regulatory exceptions (safe harbors) that, if the conditions are met, will give actors **certainty** that their practices will not be information blocking. These safe harbors include the following:

- Preventing harm (45 C.F.R. § 171.201)
- Privacy (45 C.F.R. § 171.202)
- Security (45 C.F.R. § 171.203)
- Infeasibility (45 C.F.R. § 171.204)
- Health IT performance (45 C.F.R. § 171.205)
- Content and manner (45 C.F.R. § 171.301)
- Fess (45 C.F.R. § 171.302)
- Licensing (45 C.F.R. § 171.303)

Health care providers should review the conditions of each safe harbor to see if they might apply to the provider's practices with respect to access, exchange and use of electronic health information (EHI) and take the appropriate step to modify these practices—and the policies, procedures and processes that support them—to satisfy the conditions of the applicable safe harbors. Please see the FAQ section on "How to implement compliance" for more suggestions and tips on creating an information blocking compliance program.

What if a health care provider does not qualify for safe harbor protection?

A practice that does not meet the conditions of a regulatory safe harbor does not necessarily violate the Information Blocking Rule. Rather, OIG will evaluate the practice on a case-by-case basis to assess the specific facts and circumstances (*e.g.*, whether the practice would be considered to rise to the level of an interference, and whether the actor acted with the requisite intent) to determine whether information blocking has occurred. Thus, the principal benefit of qualifying for a safe harbor is the "guarantee" that the practice does not meet the definition of information blocking and will not be subject to enforcement.[19]

What is the intent and purpose of the preventing harm safe harbor?

The preventing harm safe harbor is intended to apply to practices an actor reasonably believes will substantially reduce a risk of harm to natural persons. ONC recognizes that interference with the access, exchange or use of EHI is justified when it is to protect patients and other persons from unreasonable risks of harm. Thus, it will not be information blocking if an actor engages in practices that are reasonable and necessary to prevent harm to a patient or another person, so long as the regulatory conditions are met.

What is the intent and purpose of the privacy safe harbors?

ONC does not intend to penalize actors who cannot fulfill a request for access, exchange or use of EHI in the interests of protecting an individual's privacy. Indeed, ONC expressly recognizes that "an actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws."[20] The privacy safe harbor is, in fact, 4 separate safe harbors that apply to different privacy-related practices, such as those practices done for compliance with federal, state and local privacy laws or to honor an individual's request for greater privacy

protections. So long as the conditions of the applicable privacy safe harbor are satisfied, an actor's privacy-related practices will not be information blocking.

What is the intent and purpose of the security safe harbor?

The security safe harbor is intended to encourage best practice security protocols, increase the reliability of the health IT ecosystem and promote trust and confidence, while preventing the unreasonable and/or unnecessary interference with the access, exchange, and use of EHI. Thus, it will not be information blocking for an actor to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, so long as the regulatory conditions are met.

What is the intent and purpose of the purpose of the infeasibility safe harbor?

The purpose of the infeasibility exception is to "provide coverage to actors who face **legitimate practical challenges beyond their control** that limit their ability to comply with requests to access, exchange, or use EHI."[21] An actor may not have the technical capabilities, legal rights, or other means necessary to enable access, exchange, or use of EHI. Under such circumstances, it will not be information blocking for actor not the fulfill an EHI request, so long as the regulatory conditions are met.

What is the intent and purpose of the health IT performance safe harbor?

The purpose of the health IT performance exception is to encourage practices that are reasonable and necessary to maintain and improve health IT performance. Thus, it will not be information blocking for an actor to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, so long as the regulatory conditions are met.

What is the intent and purpose of the content and manner safe harbor?

The purpose of the content and manner exception is to give actors flexibility to fulfill an EHI request in an alternative manner from the one requested when an actor is either:

- Technically unable to fulfill the request as requested; or
- Cannot reach agreeable terms with the requestor. ONC's intent is "to support innovation and competition by allowing actors to first attempt to reach and maintain market negotiated terms for the access, exchange, and use of EHI."[22]

Thus, an actor will not engage information blocking by responding to an EHI request in an alternative manner, so long as the regulatory conditions are met.

What is the intent and purpose of the fees safe harbor?

The purpose of this exception is to allow actors to recover certain costs reasonably incurred for the access, exchange, or use of EHI, while protecting against rent-seeking, opportunistic fees, and exclusionary practices that interfere with the access, exchange, and use of EHI. Such opportunistic behaviors "reflect some of the most serious concerns that motivated" enactment of the information blocking prohibition.[23] However, it will not be information blocking for an actor to charge fees, including fees that result in a reasonable profit margin, for certain EHI requests, so long as the regulatory conditions are met.

What is intent and purpose of the licensing safe harbor?

The purpose of the licensing exception is to permit actors to license their interoperability elements to protect the value of their innovations and earn returns on their investments. So long as the regulatory conditions are met, it will not be information blocking for an actor to license interoperability elements for EHI to be accessed, exchanged, or used.

HOW TO IMPLEMENT COMPLIANCE

What do health care providers need to do to get ready for the November 2, 2020 compliance deadline?

Health care providers should:

- ✓ Start an information blocking compliance workgroup. That is, identify an organizational leader and create a multi-disciplinary information blocking compliance team (*e.g.*, legal, clinical, IT) to identify, assess, implement and advocate for organizational compliance.
- ✓ Review, update and, if necessary, create organizational policies, procedures and processes for compliance.
- ✓ Train workforce members on information blocking compliance, including assessment of workforce member knowledge following the training. Training should be ongoing and not be a one-time event. Health care providers should consider combining their information blocking training with their HIPAA compliance training.
- ✓ Implement a complaint process for identification and reporting of information blocking complaints (including anonymous reporting).
- ✓ Monitor, investigate and enforce compliance through regular risk assessments and complaint investigations. Remediate any issues, including implementing corrective action plans and disciplining workforce members, as appropriate.
- ✓ Identify and assess any vendors that exchange, use or access EHI and request confirmation of the vendor's own compliance program and confirmation that the vendor does not engage in information blocking.
- ✓ Review and amend, as necessary, contracts and agreements that impose restrictions on the other party's access, exchange or use of EHI for compliance with the regulatory safe harbors.

Remember there is no one perfect compliance program and each health care provider will need to develop their own unique compliance program that works for the provider and that the provider actually implements. Please see the FAQ section on "What will enforcement of the information blocking rule look like?" for more educational information about OIG enforcement, OIG evaluation of compliance programs and potential penalties. For more tips on how to create and implement a compliance plan, please see Health Current's Checklist for Health Care Providers: How to Create and Implement an Information Blocking Compliance Plan.

Is compliance with the Information Blocking Rule an ongoing obligation?

Yes! The November 2, 2020 deadline is the compliance start date. Compliance with the Information Blocking Rule is an ongoing compliance obligation.

What regulatory guidance materials on information blocking are publicly accessible to health care providers?

Here are some links to regulatory guidance materials published by ONC and CMS relating to information blocking compliance:

- The ONC Information Blocking Final Rule
- The OIG CMP Proposed Rule
- The ONC Information Blocking Proposed Rule
- The ONC Final Cures Act Website, which contains resource links to fact sheets and webinars. We suggest checking this website often as ONC uploads new content and guidance.
- CMS, Medicare and Medicare and Medicaid Promoting Interoperability Program Prevent of Information Blocking Attestation Fact Sheet
- CMS, The Merit-based Incentive Payment System (MIPS) Promoting Interoperability Prevention of Information Blocking Attestation: Making Sure EHR Information is Shared

Other secondary source materials include:

- The Sequoia Project, Information Blocking Compliance Resource Center
- College of Healthcare Information Management Executives (CHIME), Interoperability

ENDNOTES

[1] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25642, 25792 and 25813 (May 1, 2020).
[2] *Id.* at 25810.
[3] *Id.* at 25868.
[4] *Id.* at 25812.
[5] *Id.* at 25815.
[6] *Id.* at 25815 (emphasis added).
[7] 45 C.F.R. § 171.102.
[8] *Id.* § 171.102 (emphasis added).
[9] 85 Fed. Reg at 25799.
[10] HIPAA collectively refers to the Health Insurance Portability Act of 1996, the Health Information Technology for Economic and Clinical Health Act (HITECH), and their implementing regulations (see 45 C.F.R. Parts 160, 162 and 164, all as amended from time to time.
[11] *Id.* at 25691; 45 CFR § 171.102.
[12] ONC, United States Core Data for Interoperability USCDI Version 1 (July 2020 Errata) (last accessed September 4 2020).
[13] Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules, 85 Fed. Reg. 22979, 22985 (April 24, 2020).
[14] U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs (Update June 2020).
[15] 42 U.S.C. § 300jj-52(b)
[16] 85 Fed. Reg. at 25794.
[17] *Id.* at 25794.
[18] *Id.* at 22984.
[19] *Id.* at 25820.
[20] ONC, Cures Act Final Rule: Information Blocking Exceptions (last accessed September 4, 2020).
[21] 85 Fed. Reg. at 25867 (emphasis in original).
[22] ONC, Cures Act Final Rule: Information Blocking Exceptions, supra.
[23] 85 Fed. Reg. at 25879.