CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

Be informed.
Be involved.

Information Blocking Q/A With ONC

Last Updated: October 27, 2020

Adjudicated Questions

Q: **NEW Will ONC be providing guides or "cheat sheets" to assist providers in responding to information blocking requests outlining recommendations for how they should internally document how they responded to an information request and any exceptions they are invoking?**

A: NEW Documentation of policies and procedures is discussed in this short section of the preamble to the Cures Act Final Rule, which considers when a written policy may be helpful to ensure that a practice falls within one of the exceptions to the definition of information blocking (85 FR 25819). Some exceptions' condition[s] call for written communication with a requestor or appropriate documentation of organizational policies or particular determinations an actor may make. However, there is not a required form, template, or format for written evidence any of the exceptions.

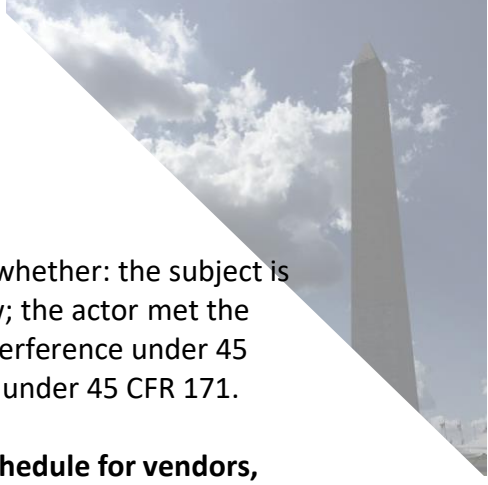
We intend for actors to have the flexibility to shape their response processes and procedures in manners most appropriate and efficient for their specific situations.

We do anticipate offering additional informational resources to help actors, such as health care providers, to plan and integrate best practices into their clinical and administrative workflows. As we develop these resources, we appreciate ongoing feedback and engagement from stakeholders. As you know, this feedback helps inform our consideration of what type of resources will be highly useful to providers and other actors.

Q: **Do information blocking provisions also apply to requests from state and local actors? For instance, if an HIE requests public health information from a hospital, but the larger provider group has elected to not join the HIE, is that considered information blocking?**

A: The information blocking regulations (45 CFR part 171) apply to a health care provider, health IT developer of certified health IT, or health information network or exchange (as defined in 42 CFR 171.102). Whether these actors' practices in fulfilling or not fulfilling requests for ***legally permissible*** access, exchange, or use of electronic health information constitute information blocking is not determined by whether the request is made by particular types of entity.

In order to determine whether a failure to report information to a public health agency would be considered information blocking, the U.S. Department of Health and Human Services (HHS) would need [to] evaluate the practice on a case-by-case basis to assess the specific facts and circumstances to determine whether information blocking has occurred.



Whether information blocking actually occurred would be based on whether: the subject is an "actor;" the claim involves "EHI;" the practice was required by law; the actor met the requisite knowledge standard; the practice rose to the level of an interference under 45 CFR 171; and the actor's practice met the conditions of an exception under 45 CFR 171.

Q: Can ONC explain more about the intersection of the certification schedule for vendors, which provides vendors until May 2, 2022 – plus 3 months (Aug 2, 2022) enforcement discretion – to deliver their customers the updates to their 2015 Edition IT for the USCDI standard and the FHIR API for patient and population services, and the CMS Promoting Interoperability Program that requires eligible hospitals and providers to attest to the following statement: I attest to CMS I am compliant with all standards, implementation specs, and certification criteria adopted at 45 CFR part 170? If a provider's vendor takes the entire time allowed to provide the updated software, that doesn't leave the provider any time for implementation and then places the provider in the situation of having a 2015 Edition that doesn't meet the certification requirements they must attest to under the CMS PI program in 2022. Are ONC and CMS working together to address this issue?

A: As this question concerns attestation statements that are required for the CMS Promoting Interoperability programs, we encourage you to direct questions related to CMS, either [to] qpp@cms.hhs.gov (for the Quality Payment Program) or qnetsupport@hcqis.org (for the Promoting Interoperability programs).

Q: Are payers considered actors?

A: For purposes of the information blocking regulations in 45 CFR part 171, the term "actor" includes health care providers, health IT developers of certified health IT, health information networks (HIN) and health information exchanges (HIE) – as defined in 45 CFR 171.102. Although health plans and other payers are not specifically identified within any of these definitions, they are also not specifically excluded. To the extent an individual or entity that is a payer also meets the 45 CFR 171.102 definition of "health care provider," "health IT developer of certified health IT" or "health information network or health information exchange," that individual or entity would be considered an "actor" for purposes of information blocking.

The *Information Blocking Actors* fact sheet on HealthIT.gov presents these definitions in an easy-to-use format.

Q: Is there a limitation by date in the regulation, or how far back in the past, that USCDI patient data has to be available to move the data?

A: Until the date specified in 45 CFR 171.103(b), an actor must respond to a request for access, exchange, or use of EHI they have with, at a minimum, the EHI requested that corresponds to any of the data elements represented in the United States Core Data for Interoperability (USCDI). After the date specified in 45 CFR 171.103(b), an actor must respond to a request for access, exchange, or use of EHI with the EHI requested that they have that meets the EHI definition found in 45 CFR 171.102.

The requirement to fulfill requests for access, exchange, and use of EHI is in any case limited to what the actor may, under applicable law, permissibly disclose in response to a particular request. However, the requirement to fulfill a request for legally permissible access, exchange, or use of EHI that the actor has is not limited to the most recent data points or to information produced before or after any particular point in time.

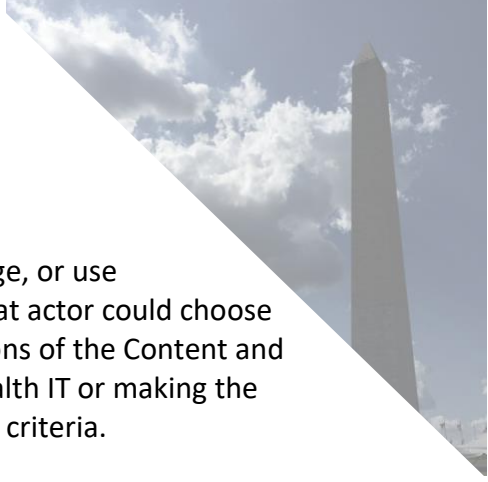
This means that the time period covered is based on what information is requested and if the information requested is information that the actor has that meets the EHI definition.

In some circumstances, such as where the actor's practice is consistent with one or more of the exceptions finalized in subpart B of 45 CFR 171, an actor's practice in not fulfilling a portion or the entirety of a particular request for access, exchange, or use of EHI may not constitute information blocking as defined in 45 CFR 171.103. If such practice came to be the subject of an information blocking investigation by HHS, HHS would evaluate the practice on a case-by-case basis, assessing the specific facts and circumstances to determine whether information blocking has occurred.

Whether information blocking actually occurred in a particular case would be based on whether: the individual or entity engaging in the practice is an "actor" as defined in 45 CFR 171.102; the claim involves "EHI" as defined in 45 CFR 171.102; the actor met the requisite knowledge standard; the practice rose to the level of an interference under 45 CFR 171; the practice was required by law; and the actor's practice met the conditions of an exception under 45 CFR 171.

Q: Are Inpatient Rehabilitation Hospitals (IRFs) subject to these rules despite not receiving any incentives to implement EMR technologies?

A: The information blocking regulations in 45 CFR part 171 apply to all individuals and entities that are actors – health care providers, health IT developers of certified health IT, or health information networks (HIN) or health information exchanges (HIE) – as defined in 45 CFR 171.102, regardless of whether they use certified technology. If an individual or entity is an actor, information blocking applies for any *electronic health information (EHI)* they may have.



If an actor is technically unable to fulfill a request for access, exchange, or use of that *electronic* ++ health information in the manner requested, that actor could choose to seek coverage of the Content and Manner Exception. The conditions of the Content and Manner Exception can be met without necessarily using certified health IT or making the EHI available in the same standards that are required by certification criteria.

The *Information Blocking Actors* fact sheet on HealthIT.gov presents these definitions in an easy-to-use format.

Q: ONC has said the Information Blocking compliance deadline is Nov 2, 2020 but we don't yet have penalties laid out by HHS for providers. Can you explain what this means for providers in-terms of compliance?

A: No actor (health care provider, health IT developer of certified health IT, or health information networks or health information exchanges) as defined in 45 CFR 171.102 is ***required*** to comply with the information blocking regulations in 45 CFR part 171 until the date specified in 45 CFR 171.101(b).

Individuals and entities meeting the 45 CFR 171.102 definition of "health IT developer of certified health IT" or "health information network or health information exchange" who are determined to have engaged in information blocking in these capacities may be subject to civil monetary penalties (CMPs) – regardless of whether they also meet the definition of "health care provider."

The timeframe for enforcement will **not** begin sooner than the compliance date in 45 CFR 171.101(b), and will depend on when the CMP rules are final. The HHS Office of Inspector General (OIG) stated in their Civil Monetary Penalty (CMP) Proposed Rule: "conduct that occurs before the effective date of our final rule will not be subject to information blocking CMPs" (85 FR 22985). Discretion will be exercised such that conduct that occurs before the CMP rule is final will not be subject to information blocking CMPs.

As of October, 2020, HHS has not yet established disincentives for health care providers or the corresponding processes for implementing such disincentives. ONC included a request for information regarding provider disincentives in our Cures Act Proposed Rule and received comments on the topic. HHS is taking those comments into consideration as the Department explores provider disincentives and corresponding processes.

CHIME Commentary: A reminder that the OIG CMP Proposed Rule does not govern providers. CHIME's continued recommendation is for providers to begin preparations to

comply with ***all*** information blocking requirements by Nov. 2, 2020. This date may be delayed by the pending COVID-19 Information Blocking Delay Interim Final Rule currently under review by the Office of Management and Budget (OMB).

Questions Awaiting Adjudication

Q: How should each actor interpret its role as an "actor" under the information blocking provisions? For instance, if a provider is also an HIE how should they interpret where they fall under the information blocking provisions?

A:

Q: Much of the discussion around APIs have been focused on getting data out of the systems, how does ONC view the ability for APIs to read information into an EHR?

A:

Q: Consumers can seek out 3rd party APIs to access the data held by actors. What certifications or standards must be applied to 3rd party APIs that are not developed or incorporated into CEHRT?

A:

Q: What role would providers have in regard to fees to access APIs to their EHRs? It seems patients have direct access to their data at no cost, but if a third-party needs access to a patient data the HIT developer can charge a fee. Can the provider charge a fee also? Do providers need to be concerned with fees in any way?

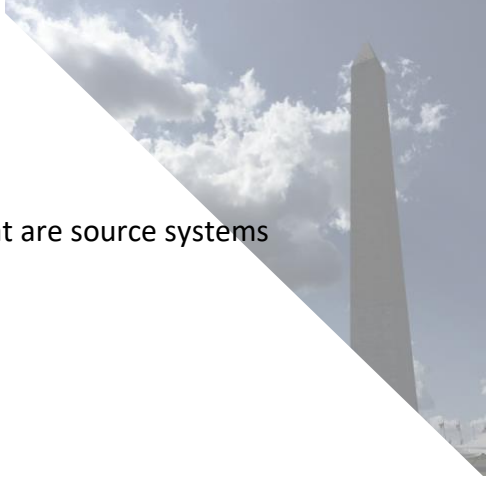
A:

Q: Many of our members are still in the throws of COVID-19 and are just starting to emerge to examine these new policies. As they absorb these policies what can you say about a glidepath to enforcement for some who may need more time?

A:

Q: Healthcare providers are facing a growing barrage of cyber threats, by one estimate the threats have increased 30,000 percent since the start of the pandemic. Can you comment on what this means for providers leery of connecting to suspicious apps?

A:



Q: How do the conditions of certification apply to niche applications that are source systems for elements of clinical data such as diagnostic vendors?

A: