the sequoia® project

Information Blocking: Detailed Q&A

Presented on a public webinar: April 17, 2020

These answers are intended as an educational resource and do not represent official ONC guidance and are not intended as legal guidance by The Sequoia Project or its contractors.

Important Information Regarding This Document:

These questions and answers were addressed in an April 17, 2020 extended Q&A Webinar on the recent ONC Information Blocking Final Rule. The questions and answers were read aloud but only questions provided during two webinars on this topic during March 2020 were presented in the webinar slides. This exclusive document, provided for the members of The Sequoia Project, is organized by question topic, and includes questions submitted before the April 17 webinar as well as all answers provided during the April 17 webinar. These answers are intended as an educational resource and do not represent official ONC guidance and are not intended as legal guidance by The Sequoia Project or its contractors.

TABLE OF CONTENTS

1.1. Who do the Rules Apply to: HIE/HIN, Providers, Payers, etc.?

1.1.1 How does this rule apply to payers (e.g., health insurance companies)? Does information blocking apply to payers as well as providers? Generally hoping to learn more about how payers are impacted.

Response:

Payers are not a defined category of information blocking actor. In the Final Rule, ONC declined to exclude certain categories of organization, such as payers, from the HIE/HIN definition. A payer might have lines of business that qualify it as an actor, for example acting as a provider or as an HIE/HIN. If so, it appears that the payer's activities in those specific lines of business may qualify the payer as an actor subject to information blocking compliance for those functions, where the organization controls interoperability elements for access, exchange, or use of EHI.

Similarly, ONC in the NPRM states that a provider organization could also qualify as an HIN if it exercises control over HIE/HIN functions, but only for the HIN functions; it would be treated as a provider when it functions as a provider. This is a somewhat different issue than the scenario of developer organizations, whose lines of business subject to information blocking are not limited to the certified health IT.

Overall, it appears that ONC will focus on the actions of an organization that align with one of the actor categories and not apply all actions of the organization to that single category.

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

Response:

Response: ONC does not focus on whether a direct patient provider relationship exists but rather whether an organization controls interoperability elements relating to access, exchange, or use of EHI.

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

Response:

Information blocking requirements are not limited to organizations with data subject to HIPAA so long as they meet the category of actor. ONC is clear that the definition of EHI as HIPAA-defined ePHI in a Designated Record Set (DRS) is not limited to actual HIPAA covered entity held ePHI.

ONC states that *". . . the reference to the three types of activities does not limit the application of the HIN/HIE definition to individuals or entities that are covered entities or business associates (as defined in HIPAA)."* (p. 624). In addition, ONC states that*: "We have defined EHI (§ 171.102) to mean electronic protected health information (ePHI) as the term is defined for HIPAA in 45 CFR 160.103 to the extent that the ePHI would be included in a designated record set as defined in 45 CFR 164.501 (other than psychotherapy notes as defined in 45 CFR 164.501 or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding), regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103."*

1.1.4 Do Public Health programs meet the definition of an HIE/HIN and therefore become subject to the information blocking requirements?

Some programs (e.g., immunization registries) collect data from multiple sources (multiple provider organizations) and share with providers. Does this qualify as facilitating exchange by more than two entities?

I'd like to hear if Public Health programs meet the definition of either an HIE or an HIN and are subject to the requirements of information blocking. Some programs, such as immunization registries, do collect data from multiple sources and share it.

Response:

It depends. First, a public health program would need to exchange data for treatment, payment or operations as defined by HIPAA in order to be an HIE/HIN. If it does, according to ONC in the Final Rule and as explained in public presentations and webinars, the next key question is whether the providers who share information with the public health program are also using the public health program to exchange with each other. If they are not, the public health program is not operating as an HIE/HIN.

1.1.5 Clearinghouses exchange far more data than just claims. Does the exclusion of clearinghouses from the definition of an HIE/HIN include any information exchanged by health care clearinghouses, or just claim data?

Response:

The focus of the general exclusion of clearinghouses seems to be the nature of the exchange (i.e., is it a "traditional clearinghouse function") and not the nature of the data, for data that otherwise

These answers are intended as an educational resource for our members and do not represent official ONC guidance and are not intended as legal guidance by The Sequoia Project or its contractors.

meets the definition of EHI. The issue is primarily whether the providers who share information with the clearinghouse are also using the clearinghouse to exchange data with each other.

1.1.6 How does the rule apply to multi-specialty physician groups?

Response:

Group practices (and many of their clinicians) are identified as Providers in the Final Rule and subject to requirements and enforcement requirements for providers, which to date appear to stem from attestations for CMS incentive programs like MIPS. Note that the current CMS attestations, while presented by CMS under the label of "Prevention of Information Blocking Attestation," do not actually reference that term as defined in Cures or by ONC in the Final Rule, but rather focus on two general questions backed by three specific attestations, asking whether the provider acted in good faith to: support the appropriate exchange of electronic health information and did not knowingly and willfully limit or restrict the compatibility or interoperability of the Certified EHR.

1.1.7 Please address examples of entities meeting the new definition of HIE/HIN.

Response:

ONC focuses on functional activities rather than examples of specific entities and to date has avoided entity-focused examples, although noting that it might provide more detailed guidance and even advisory letters in the future. ONC does provide examples of entities not expected to be HIEs/HINs and clarifies that an HIE/HIN must facilitate exchange among more than two unaffiliated individuals or entities, besides HIN/HIE, that are enabled to exchange with each other.

This revision is intended to ensure that the definition does not unintentionally cover "essentially bilateral exchanges" in which the intermediary "simply" performs a service on behalf of one entity in providing EHI to one or more entities and no "actual exchange" occurs among all entities (e.g., acting as intermediary between two entities where first sends non-standardized data to be converted by intermediary into standardized data for receiving entity).

ONC notes that the narrower definition of HIN/HIE should "clearly exclude entities that might have been included under proposed definitions (e.g., social networks, ISPs, and technology that solely facilitates exchange of information among patients and family members)" and in public discussion has stated that the revised definition excludes "traditional claims clearinghouse functions".

1.1.8 How can HIEs/HINs be held to a higher standard that the providers? They are the Covered Entities, we are Business Associates, and we can only share data in accordance with our contracts and BAA terms.

Response:

First, the differential information blocking standards for HIEs/HINs and Providers were specified by the Congress in 21st Century Cures, so ONC had no choice but to carry these through to the Final Rule. Second, ONC does not require actors to violate their BAAs, which may limit their data sharing, although it also notes that such BAAs could reflect and represent information blocking. On a related matter, ONC focuses on EHI and interoperability elements controlled by the HIE/HIN or another actor.

1.1.9 I am interested in HIE requirements and how HIE supports new rulings.

I am curious about what must an HIN/HIE do to be compliant in ways of sharing data - CCDA or FHIR with data elements specified in USCDI is my understanding.

It is clear that HIN/HIEs are actors in Information Blocking. However, most do not do Certification. If they do not do Certification, must they still support USCDI? In one or both of FHIR and CCDA? Or in "some standard format"?

Response:

Clearly HIE as a verb is critical to data liquidity and preventing information blocking. HIEs as a noun are, as stated, one of the actor categories based on their specific functions. In general, an HIE would not be required to adopt or use specific technical approaches or standards, whether USCDI or CCDA or FHIR, as they are not subject to ONC certification or CMS incentive programs. At the same time, the use of non-standard approaches can implicate information blocking and the Content and Manner exception looks to ONC and SDO standards in its hierarchy of "manners" of responding to request for EHI. So, overall, it would behoove HIEs to use standards like CCDA and FHIR, including ONC-adopted versions, as well as the USCDI, to be greatest extent possible. Where they are unwilling or unable to do so, it would be important to have and document well-founded reasons.

2.1. EHI and USCDI

2.1.1 If the USCDI doesn't have to be implemented for 24 months after publication of the Final Rule, what does it mean that information blocking scope is restricted to EHI (defined as USCDI data elements) for the first 24 months after publication of the Final Rule (e.g. if provenance isn't implemented until the 24 months, is it information blocking if provenance isn't implemented at month 6?

In the Final Rule (beginning on page 59 and again on page 101), with respect to the API requirements – it appears that six months after the publication of the final rule, systems much be able to access and exchange codes from within the USCDI definition. The timeline for certification compliance with the USCDI definition is 24 months from the date of publication.

Do the API requirements mandate that ALL USCDI codes must be available to access and exchange at the six-month compliance date or only that all codes available to access and exchange at that time must be from within the USCDI definition? Additionally, if the interpretation is that all USCDI codes must be available at the six-month date of compliance, should developers be seeking a Content and Matter exception until they complete the full transition to the USCDI specifications.

Response:

The USCDI, including specified standards, does not need to be implemented into certified health IT for 24 months after publication of the Final Rule. However, the data elements in the USCDI (but not specific codes and standards) are in force for information blocking six months after publication. These would include "provenance" as a data element but not the ONC specified standards for provenance.

If specific data elements (or specific data) are not available in EHI controlled by the Actor, it appears that they would not be subject to an information blocking complaint for those data elements. The focus of information blocking is enabling access, exchange or use of data that is controlled by an actor. So, a Content or Manner exception may be appropriate for any actor who cannot meet a request in the manner specified if that includes the full USCDI definition.

For interoperability elements, ONC states that "[w]e have finalized the definition of 'interoperability element' to mean hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that: (1) may be necessary to access, exchange, or use EHI; and (2) is controlled by the actor, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of EHI." (p. 641)

2.1.2 How much legacy EHR data is a hospital required to provide through APIs if only some discrete data were converted to the current EHR and the rest is in PDF format (chart export from the old EHR). We're assuming all data under the USCDI but would like opinions.

Response:

First, specific <u>hospital</u> API data element requirements would come from CMS incentive program API requirements. Requirements for API access would likely mostly focus on available data in electronic form that is in the USCDI (or the CCDS now). We suggest that you look to current CMS requirements here. For information blocking, there is no specific API requirement, other than discouraging use of non-standard interoperability elements, and the Content and Manner and Infeasibility exceptions would come into play for such legacy data, for which alternate means of availability might be needed.

2.1.3 What are the designated record sets per HIPAA that are required to be shared by providers and other actors at 24 months after publication? What are technologies that must be used to share this greatly expanded set of data?

Response:

ONC defines EHI to mean electronic protected health information (ePHI) as defined for HIPAA to the extent that the ePHI <u>would be included in a designated record set</u> as defined in HIPAA with some exceptions as discussed in the last webinar, <u>regardless of whether the group of records are used or maintained by or for a covered entity</u>.

The Designated Resource Set as defined in the Privacy Rule as:

I. A group of records maintained by or for a covered entity that is:
   a. The medical records and billing records about individuals maintained by or for a covered health care provider;
   b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
   c. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

II. The term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

With respect to technologies, for certified health IT, and those who must use certified health IT, the minimum technology to be available is the USCDI, FHIR 4.0.1 APIs and associated standards and implementation guides specified by ONC. But, as indicated previously for information blocking more broadly, EHI is broader than USCDI and there is no specific API requirement or other technology, other than discouraging use of non-standard interoperability elements, and the Content and Manner and Infeasibility exceptions would come into play for technology to access EHI.

2.1.4 Information blocking will take effect 6 months after publication. Is the expectation to exchange using the USCDI as the minimum requirement? Is the Common Clinical Data Set (CCDS) still viable until it is ready?

Response:

Yes, the expectation is to use the data elements in the USCDI but not the associated standards and code sets. The CCDS would continue in place for certified health IT and its users until the USCDI is fully implemented.

3.1. Standards

3.1.1 When will the FHIR 4 standards be supported? Does this include everyone connected? Will real time transactions be supported? Will research type queries be supported (no patient specific)?

Response:

For ONC certified APIs, FHIR 4.0.1 must be supported 24 months (extended by three months by recent ONC enforcement discretion) after publication of the Final Rule. The specific requirements only covers developers and users of certified health IT. The expectation is that the FHIR APIs/apps would be able to work in real time. It does not appear that research queries are explicitly supported but the certification requirements do include the FHIR multi-patient bulk data implementation guide.

4.1. Access Exchange, and Use

4.1.1 Please explain "write" access requirements on API information blocking? Isn't it "read-only"?

Response:

The requirement for the revised API technical certification requirements includes only "read" access. The definition of "use" includes "write" access without reference to specific technical standards and requirements, subject to the applicability of exceptions like Content and Manner or Infeasibility.

4.1.2 What is the true impact for HIEs that do not have patient access to portal in terms of API requirements?

Response:

HIEs that do not have ONC-certified APIs do not need to implement APIs, FHIR-based or otherwise, but they must respond to requests for access, exchange, or use consistent with the interoperability elements that they control for EHI and the “manner and content: and “infeasibility” exceptions. Note that an HIE/HIN that is also a CMS-regulated health plan would have API requirements for its health plan functions.

5.1. Information Blocking

5.1.1 If a state HIE asked the hospitals in that state to participate (and offered to cover associated expenses), and the hospitals declined, would this action by the hospitals be considered information blocking?

Response:

It is unclear whether failure to participate in an HIE per se would be considered information blocking; we tend to think not. But if the failure resulted in not responding to authorized requests for access, exchange, or use, it could be information blocking.

5.1.2 If a group of providers refused to permit an HIE to provide de-identified data for evaluation of a program or service of a provider, does that refusal constitute data blocking?

Response:

De-identified data does not qualify as ePHI or EHI, so no.

ONC states that “[w]e agree that health information that is de-identified consistent with the requirements of 45 CFR 164.514(b) should not be included in EHI. It is not, however, necessary to specifically exclude such de-identified information from the EHI definition because information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable information, so it would not be EHI (see 45 CFR 164.514(a)). To note, once PHI has been de-identified, it is no longer considered to be PHI. So, such information would not be considered EHI by definition (see 45 CFR 164.514 (b)).” (p. 532)

5.1.3 If providers refused to permit an HIE to send batch downloads of patient information for purposes of quality measurement, would that be data blocking?

Response:

It could be. Clearly ONC intends for batch access to be supported by certified HIT and this kind of access is a priority. It appears that failure to honor a request for access, exchange, or use of batch data would be subject to the same analysis as such a failure for a single patient's data, so long as the HIE has a right under state or federal law to such data.

5.1.4 If organizations refuse to do setup for Summary of Care measures, is that information blocking?

Response:

The intent of the question is a bit unclear without further information. If the setup is needed to achieve access, exchange or use of EHI, refusal to do setup to achieve such access could be information blocking but we don't think that failure to support the MIPS measures would be.

5.1.5 Some hospitals are only sending ADTs and not sending other data types to their HIEs, will this be considered as information blocking?

How are hospitals who are currently sending ADT data to HIEs impacted?

Response:

HIEs often accept ADT feeds from their hospital participants to help build a patient centric data repository to support query/retrieve. This exchange is addressed in the HIE data sharing agreement and by itself, would not violate the Information Blocking Rule. If a hospital refuses to send information to an HIE with which it has a data sharing agreement that would allow sending such information, such a refusal could implicate information blocking, subject to the exceptions and a case/fact-specific analysis.

More generally, hospitals sending ADTs would not be specifically affected or not affected. Likely issues relevant to ADT and information blocking could be any fees associated with ADT notifications and any discriminatory or anti-competitive policies for provision of notifications to HIEs or others.

5.1.6 Would a clinical registry operated by a third-party, such as a health care quality collaborative operating a clinical registry and offering quality measurement and reporting services to provider entities (i.e., healthcare operations), generally not be considered an HIN/HIE and fit the criteria of bilateral exchange?

Response:

Likely yes, as long as the registry is not facilitating exchange among providers who submit to the registry.

5.1.7 How do we expect requests to come through from third party developers and from patients?

Response:

We expect multiple types of requests, which could be with the same methods used now and increasingly, from an app looking to connect with a healthcare organization's APIs as well as directly to developers. ONC specifies certain relationship flows for certified APIs but the broader information blocking request flows are likely to be varied.

5.1.8 I need proper understanding of information blocking and how that affects HIE's and more detail around the exceptions.

Response:

We suggest that you refer to the March Sequoia Project webinar, publicly available on The Sequoia Project information blocking resources page, as well as the excellent ONC resources.

5.1.9 Given a feasible request for EHI where no exception is provided- could you comment on what is expected to be a reasonable timeframe for an actor to exchange requested EHI? At what point could an actor be capable of info blocking if the request is delayed?

Response:

ONC mixes qualitative and quantitative timeliness criteria.

For information blocking, ONC states that is has "not established a set timeframe for what 'timely' access means because there is so much variability regarding what 'timely' will mean based on the specific facts and circumstances, and particularly with regard to the broad scope of health IT being discussed. . . whether access is considered timely will be determined based on the specific facts and circumstances." ONC refers readers of the Final Rule to the discussion on "Limiting or Restricting the Interoperability of Health IT" where it discusses how slowing or delaying access, exchange, or use of EHI could be information blocking.

These answers are intended as an educational resource for our members and do not represent official ONC guidance and are not intended as legal guidance by The Sequoia Project or its contractors.

For the Infeasibility Exception, ONC states that responses to requests for data access, exchange, or use must be within 10 business days. For EHI Export, ONC states that "…'timely' means near real-time, while being reasonable and prudent given the circumstances."

6.1. Privacy and Security Exceptions

6.1.1 How does the 2nd bullet on Slide 31 (of the March webinar) jibe with the Privacy Exception Precondition not satisfied: If an actor is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing access, exchange, or use?

Response:

The second bullet states that the "Information blocking provision may require actors to provide access, exchange, or use in situations where HIPAA Rules would not require access of similar information; the HIPAA Privacy Rule permits, but does not require, covered entities to disclose ePHI in most circumstances." This is a general characterization by ONC of how the Information Blocking provisions interrelate with and shift the impact of HIPAA. But the specific Privacy exception precondition cited holds. In a sense, this precondition indicates that an actor can indicate that it is not permitted to provide access, exchange, or use. See also the prior bullet on page 30 of the initial presentation, "Actors need not provide access, exchange, or use of EHI in a manner not permitted under the HIPAA Privacy Rule."

6.1.2 Could state laws conflict with information blocking objectives, and if so, how should HIEs properly document that certain sensitive data (i.e. HIV, SUD) must be blocked to remain compliant with either state laws or contractual agreements?

Response:

Any information blocking requirement is subject to state laws, which provide one basis for the Privacy Exception. ONC does not provide documentation requirements but, for the Privacy Exception, does reference HIPAA and OIG documentation requirements.

6.1.3 Can you speak specifically to the exchange of sensitive data, including both behavioral health and substance use data?

Response:

Exchange of such data may, in some cases be subject to specific federal and state laws and regulations, for example 42 CFR Part 2. It is important to recognize that not all behavioral health data is subject to protections beyond what HIPAA applies generally to PHI. ONC addressee some of the relevant issues with the Harm Exception.

7.1. Fee Exception

7.1.1 Why is the language in 171.301(b)(2) regarding fees being prohibited for electronic access of an individual's EHI by "another person or entity designated by the individual" not in conflict with the recent DC District Court decision on the Ciox v. Azar case related to fees charged to third parties it which an individual directs his/her health information be transmitted?

The nuance may be the definition of electronic access in Part 171: to mean an internet-based method that makes the EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request. If this is not the type of access requested by the individual, the HIPAA fee decision of the court may apply.

If I was a lawyer that did malpractice cases, I would procure a consumer-facing app that uses FHIR R4 and provide that to my client to access the client's EHI.

Response:

It appears that the identified nuance may be correct based on a recent ONC webinar, focusing on a strict definition of “no special effort” as no manual effort needed. ONC has not addressed the Ciox issue directly but appears to be basing its regulatory provisions on the authority granted by Cures and not HIPAA.

On p. 957, ONC states that “[f]or purposes of the Fees Exception, we define electronic access [by a patient to their EHI] to mean an internet-based method that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request (§ 171.302). We discussed the meaning of “electronic access” in the Proposed Rule (see 45 FR 7540). We have defined “electronic access” in this final rule consistent with the Proposed Rule, including distinguishing it from the methods and efforts we cited in the Proposed Rule that we did not consider electronic access and for which a fee could be charged (see 45 FR 7540).”

7.1.2 Is cost considered in the blocking of interoperability? Will cost of integration be considered in data blocking definition?

Response:

Yes, cost, including integration costs under an actor's control, can be a factor that implicates information blocking and addressed as part of Fee and Licensing exceptions.

8.1. Business Associates Agreements (BAAs)

8.1.1 What wording should we pay attention to in our business associate agreements? What are red flags?

8.1.2 Response:

First, if you are a business associate and also an actor, you will want to be mindful of any limitations on your disclosure in response to requests for EHI to which you have access as a business associate. ONC states that it does not expect actors to violate BAAs. At the same time, ONC states that a BAA or its service level agreements (SLAs) must not be used in a discriminatory manner to forbid or limit disclosures permitted by Privacy Rule. It also states that both actors who are BAA parties are subject to information blocking provisions.

9.1. Organizational Policies and Contracts

9.1.1 What type of policies do you recommend having in place to address Information Blocking for EHRs?

Response:

Developers will need policies to implement the information blocking related policies in the ONC Conditions of Participation, including those that relate to API access and fees. They will also want to ensure that they have policies to address practices that may implicate information blocking, identification of relevant exceptions, review of BAAs and contracts, and policies to ensure timely internal communications and issue alerts.

9.1.2 I'm interested in learning about Sequoia's thoughts on how organizations might go about updating existing health IT contracts to ensure compliance with information blocking exceptions.

Response:

It will be important to review contracts to identify any fee, licensing or other provisions that could implicate information blocking. It would be important, as well, that such contracts support applicable information blocking exceptions.

You will want to ensure that your inside and outside counsel are familiar with the information blocking statute and regulations. It will also be important that enforcement of contracts that have problematic provisions is adjusted for information blocking obligations even if the contracts have not been revised and renegotiated. Make sure you address BAAs as well (so that these cannot be construed as information blocking) as well as SLAs, the latter of which will be relevant to use of the Performance exception.

ONC is clear that "contracts and agreements can interfere with the access, exchange, and use of EHI through terms besides those that specify unreasonable fees and commercially unreasonable licensing. For instance, a contract may implicate the information blocking provision if it included unconscionable terms for the access, exchange, or use of EHI or licensing of an interoperability element, which could include, but not be limited to, requiring a software company that produced a patient access application to relinquish all IP rights to the actor or agreeing to indemnify the actor for acts beyond standard practice, such as gross negligence on part of the actor. Such terms may be problematic regarding information blocking in situations involving unequal bargaining power related to accessing, exchanging, and using EHI."

For developers, ONC states (about the Communications Condition of Certification), that "[a] health IT developer must not impose or enforce any contractual requirement that contravenes the requirements of this Condition of Certification. Furthermore, if a health IT developer has contracts/agreements in existence that contravene the requirements of this Condition of Certification, the developer must notify all affected customers, other persons, or entities that the prohibition or restriction within the contract/agreement will not be enforced by the health IT developer. In response to comments, we have finalized in § 170.403(b)(2)(ii) that health IT developers are required to amend their contracts/agreements to remove or make void such provisions only when the contracts/agreements are next modified for other purposes and not within the proposed period of time from the effective date of this final rule." (emphasis added) You will also want to ensure that agreements with contractors do not implicate information blocking and support applicable exceptions and ONC provides examples of information blocking in which contracts have information blocking implications.

10.1. Implementation and Enforcement Dates

10.1.1 When is the final ruling on this going to be done?

Does it seem likely that the Rules will be delayed being published in the Federal Register and therefore the timeline for industry implementation and adherence may also be delayed?

Are there any changes to the critical deadlines given competing resources due to COVID-19?

Has any consideration been given to pushing out any dates due to COVID-19 activities?

Response:

(Updated for recent ONC actions) The ONC and CMS Final Rules were formally published in the Federal Register on May 1, 2020. the event that starts the clock to compliance. This delayed publication may have been due, in part, to industry challenges from the pandemic. In addition, both ONC and CMS have announced some implementation delays in the form of pandemic-related "enforcement discretion". For ONC, certification-related provisions, including those that address information blocking, were pushed out by three month, but the information blocking compliance date of six months after publication in the Final Register (i.e., November 1, 2020) was not changed.

Also, on April 24, 2020, the HHS Office of the Inspector General (OIG) published a proposed Rule regarding OIG enforcement of Civil Monetary Penalties (CMPs) for information blocking (for developers of certified health IT and HIEs/HINs). There is a 60-day comment period on this proposed rule and OIG has proposed an enforcement date (subject to comments) of 60-days after its eventual Final Rule on information blocking CMPs.

10.1.2 My understanding from the briefing at the March HITAC is that the compliance date for information blocking per se is not tied to when the OIG's enforcement and CMP rule is final.

The actual enforcement of the information blocking provision and CMPs may be delayed and the rule indicates enforcement would be no earlier than the 6-month compliance date. It was not very clear in the rule and ONC should clarify this in an FAQ.

One could say a compliance date that has no enforcement in effect is equivalent to a compliance delay. For a health care provider, getting started on coming into compliance with the Information Blocking provision sooner rather than later is better now that the rule is out.

When will the penalties be in effect?

Response:

Compliance with the information blocking provisions is required six months after the Final Rule publication date (i.e., November 1, 2020). Civil Monetary Penalties are in effect the later of six months after the publication date of the ONC Final Rule or the effective date of an HHS OIG Final Rule on Civil Monetary Penalties (CMPs). ONC has noted that a compliance date (i.e. from the ONC Final Rule) can be sooner than an enforcement date (i.e.., as dictated by the timing of the OIG Final Rule).

On April 24, 2020, the HHS OIG published a Proposed Rule regarding OIG enforcement of CMPs for information blocking (by developers of certified health IT and HIEs/HINs). OIG has proposed an enforcement date (subject to comments) of the later of 60-days after its eventual Final Rule on information blocking CMPs or the ONC compliance date of November 1, 2020.

It appears that provider-related enforcement would also be linked to the ONC-designated compliance date for actors of six months after publication. At the same time, both ONC and especially the OIG (in its proposed rule) emphasize that "additional disincentives" for providers based on referral by the OIG to an "appropriate" HHS agency will depend on subsequent HHS rule-making.

Current information blocking obligations for providers that could be associated with penalties or other disincentives appear to stem from attestations for CMS incentive programs like MIPS. The CMS attestations, while presented by CMS under the label of "Prevention of Information Blocking Attestation," do not reference that term as defined in Cures or by ONC in the Final Rule, but rather focus on two general questions backed by three specific attestations, asking whether the provider acted in good faith to: support the appropriate exchange of electronic health information and did not knowingly and willfully limit or restrict the compatibility or interoperability of the Certified EHR.

10.1.3 Please further discuss issues associated with enforcement (ONC & OCR) especially related to Individual Rights.

Response:

Enforcement with respect to the HIPAA individual right of access could fall to CMS (for providers who attest that they do not engage in information blocking), OIG for providers (re: attestation), developers and HIEs/HINs relative to information blocking provisions that relate to the individual right of access, ONC as it relates to developer information blocking assurance and attestations, and the HHS OCR as it relates to general enforcement.

11.1. General Suggestions

11.1.1 Would love to hear real stories, initial experiences, if any, about the implementation of this policy.

Response:

We agree and will be facilitating gathering and disseminating such information to the community and to ONC.

11.1.2 Interested in knowing what provider organizations need to be aware of, related to information blocking.

Response:

We have tried to address some of these issues in our initial webinar and today. This information will be a priority as we go forward. It is also important to recognize that any additional provider "disincentives" for information blocking, if any, have yet to be determined.