

21st Century Cures Act Information Blocking Rule: Implementation and Implications for Family Planning Programs

August 3, 2021
Transcript

Slide 1



21st Century Cures Act Information Blocking Rule

Implementation and Implications for
Family Planning Programs

August 3, 2021 | 3–4 p.m. ET



Jillian Maccini: All right. Hello everyone, this is Jillian Maccini with the Reproductive Health National Training Center, and I'm delighted to welcome you all to today's webinar about the 21st Century Cures Act Information Blocking Rule. A few announcements before we begin, everyone on the webinar today is muted, given the large number of participants. Also, we'll have a Q&A at the end of the webinar. Today, many of you submitted questions with your registration. So we will begin with those questions. If you have other questions, you can ask those using the chat at any time. Also, a recording of today's webinar, the slide deck and a transcript will be available on RHNTC.org within a few days.

Slide 2

Introduction



Jillian Maccini, MBA
(she/her)
RHNTC TA Provider
Consultant @ JSI, based in NC



Abigail English, JD (she/her)
Legal & Policy Consultant in Adolescent
& Young Adult Health
Director, Center for Adolescent Health &
the Law



The information presented today is for educational purposes only and not intended to be legal advice for any specific entity. All primary sources should be reviewed to ensure comprehensive understanding as well as to keep up with any and all changes and clarifications.

As mentioned, I'm Jillian Maccini, I'm a consultant at JSI, based in North Carolina, and a TTA provider for RHNTC. I'm joined by Abigail, who's a lawyer, researcher and advocate for the rights of vulnerable young people. For more than 20 years, Abigail has run the Center for Adolescent Health and the Law in Chapel Hill, North Carolina. Prior to founding the Center for Adolescent Health and the Law, she was an attorney at the National Center for Youth Law in San Francisco.

Slide 3

This webinar was supported by the Office of Population Affairs (Grants FPTPA006030, TPSAH000006) and the Office on Women's Health (Grant ASTWH2000-90-01-00).

The views expressed do not necessarily reflect the official policies of the Department of Health and Human Services; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.



Disclaimer

This presentation was supported by the Office of Population Affairs, OPA, and the Office on Women's Health. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of OPA, OWH or HHS. Further, the information presented today is for educational purposes only, and is not intended to be legal advice for any specific entity. All primary sources should be reviewed to ensure accuracy as well as to keep up with any and all changes and clarifications. The implementation of the rules and policies that we're discussing today is fairly new, as the rule has only been in effect for a couple of months, and so evolution is likely. Citations and further reading are provided on almost every slide to guide you in where to find that primary source information and additional information.

Slide 4

Learning Objectives

By the end of the webinar, participants will be able to:

1. Provide a high-level overview of the 21st Century Cures Act Information Blocking Rule, including whether it pertains to family planning programs.
2. Describe at least two of the exceptions to the Information Blocking Rule.
3. Identify at least two steps or actions important to complying with the Information Blocking Rule.



Our goal is that by the end of the webinar today, participants will be able to, one, provide a high level overview of the 21st Century Cures Act Information Blocking Rule, including whether it pertains to family planning programs. Two, describe at least two of the exceptions to the information blocking rule, and three, identify at least two steps or actions important to complying with the information blocking rule. So to get us started today, we're going to do a poll, and we would like to know how would you rate your current level of knowledge regarding the information blocking rule in the 21st Century Cures Act?

You're going to rate yourself between one and five, one being little to no knowledge, two, some knowledge, three, knowledgeable, four, very knowledgeable and five expert. I love the level of participation we have here. Thank you. Great, I think we can close the poll. So, seven out of 10 of you have said you have little to no knowledge, while the others are, three out of 10 are somewhere between some knowledge and knowledgeable. Thanks so much for sharing that, hopefully by the end of this, we will be able to move several of you or most of you up to at least that three.

Slide 5

What is Information Blocking?

Information Blocking refers to a rule in the Office of the National Coordinator for Health Information Technology's (ONC) [21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program](#).

The Final Rule prohibits **actors** from **blocking the exchange** of **electronic health information** and seeks to increase the ease and choices available for patients to access their data.

So just a couple of terminology notes before we get started, I will refer to clinics and patients here to be somewhat consistent with the regulations. I know client is the vernacular that's more typically used in family planning. But these rules refer to patients and refer to health care providers that's using the terms patients and clinics. So let's get started with what exactly is information blocking. Information blocking refers to a rule in the Office of the National Coordinator for Health Information Technology known as ONC. So when I say ONC, that's what I'm referring to.

In ONC's 21st Century Cures Act, interoperability information blocking in the OnC health IT certification program. The final information blocking rule prohibits actors from blocking the exchange of electronic health information and seeks to increase the ease and choices available for patients to access their data. ONC released the final rule, which we are referring to throughout in March of 2020. The final rule was pushed back several months from its initial effective date as a result of COVID, but the final rule went into effect April 5th of 2021. So it's now been in effect for about four months. The three terms bolded and in color on this screen, which are blocking the exchange, actors and electronic health information, will be defined in further detail in coming slides.

Slide 6

Definition: Blocking the Exchange of Information

Blocking the exchange of electronic health information (EHI) means business, technical, and organizational practices that prevent or materially discourage the access, exchange or use of EHI when an Actor knows that these practices are likely to interfere with access, exchange, or use of EHI. If by a healthcare provider, there must also be **knowledge that such practice is unreasonable and likely to interfere with**, prevent, or materially discourage access, exchange, or use of EHI.

Source: American Medical Assoc. Part 1: What is information blocking?

The first term to understand is what blocking the exchange of information means, blocking the exchange of electronic health information or EHI means practices that prevent or materially discourage the access, exchange or use of EHR. So, first thing to note is that blanket policies that disallow the sharing of information broadly are primary example of this, or essentially anything that's a barrier to a patient accessing their electronic health information. The American Medical Association or the AMA, highlights the following examples of information blocking among EHRs, things like restrictive and unfair contractual limitations on providers use and exchange of medical information, excessive fees charged to create EHR interfaces or connections with other health information technology, and non standard methods of implementing EHRs and other health IT that block the access exchange or use of medical information.

Non standard methods of implementing EHR means things like not using available features that could facilitate access, such as shutting off the patient portal, which is an example many people have heard. Note that this definition refers to the access, exchange and use of EHI, so let's parse those out a little bit more. Access is the ability or the means necessary to make EHI available for exchange, use or both. Exchange is the ability for EHI to be transmitted between and among different technologies, systems, platforms, networks, et cetera, and then use is the ability for EHI to be understood and acted upon once accessed and exchanged, and acted upon here means including the ability to read and write and it's also bidirectional.

Note that this statement says in part when an actor knows that these practices are likely to, ONC notes that the knowledge standard varies based on the type of actor. For healthcare providers, the standard is that the actor knows that such practice is unreasonable, and is likely to interfere with access, exchange or use of electronic health information.

Slide 7

How does this relate to other privacy laws?

Information blocking rule differs from HIPAA and other existing rules in that they defines the only things/situations where information is not to be shared, with the *implicit* requirement that **EHI is to be shared in all other situations** for the purposes of patient access.

The information blocking rule only provides eight exceptions or situations in which an actor is permitted to "block" the sharing of information.

For full details review the [Information Blocking Exceptions](#) fact sheet

So let's touch on HIPAA for a moment, the privacy, security and Breach Notification Rules under the Health Insurance Portability and Accountability Act of 1996, known as HIPAA, were intended to support information sharing by providing assurance that sensitive health records would be maintained securely and shared only for appropriate purposes, or with express authorization of the patient.

Although the regulations have been in effect for quite some time, healthcare providers and entities still frequently question whether the sharing of health information, even for routine purposes like treatment or care coordination is permissible under HIPAA. Confusion or what is sometimes referred to as over interpretation of privacy rules has been cited by many as an obstacle for interoperability or for the sharing of electronic health information. This confusion and obstacle was partially the impetus for this particular part of the 21st Century Cures Act, along with other changes such as transition from meaningful use to promoting interoperability.

A couple of key notes to understand is that each regulation, for example, this information blocking rule that we're talking about here today, HIPAA, 42 CFR Part Two, which you may be less involved with, and or state laws, each applies only to specific types of entities who meet the definition set forth in each, and similarly each has its own definition of what information or records are covered by the rule or statute. Information blocking rules do not supersede rules such as the prohibitions that are in place under 42 CFR Part Two, for substance use disorder programs or state laws that require additional specific consent for sharing of things like HIV related information for example.

Similarly, the information blocking final under the information blocking final rule, actors are not required to violate business associate agreements otherwise known as BAAs or service level agreements required

under HIPAA. However, these contracts cannot be used in a discriminatory manner by an actor to forbid or limit disclosures that would otherwise be permitted under the information blocking rule, meaning that it can't say that you and I will share information but you're broadly prohibited from further sharing, for example. The information blocking rules do allow for verifying the identity or authority of a person or entity requesting access to EHI, as required by law or specified in existing statute. The information blocking rule spells that out in the text of the final rule.

Then finally, the information blocking rule provides eight exceptions or situations in which an actor is permitted to block the sharing of information. We'll get into that a little bit later.

Slide 8

**Information Blocking rule
requires that actors provide
ongoing access, exchange,
and use when requested.**

Responsive to requests for patient access. Other privacy laws typically require proactive actions to secure data and protect against disclosure.

So first, information blocking requires being responsive to requests for access. These requests can come from the patient or from a provider requesting access for patient care or quality of improvement, among other entities, which we'll discuss a little bit more later. Note that these are not one and done requests, but rather requests for ongoing continuous access, exchange, and use and or use. It's also important to note that this does not mean a written request to your agency, that's not what we're talking about here.

It means a request for access in the form of generally something electronic, something like signing up for and signing into the patient portal, or using functionality that would otherwise permit the sharing of the patient's health record with another provider. One example of this, is share everywhere. Note that under the information blocking regulations, the actor is only required to fulfill a request with the requested EHI that they have and that they can permissibly disclose to the requester under applicable law. However, for protected health information that an actor has but doesn't maintain electronically, all HIPAA requirements would still be applicable.


So I say all that to say that HIPAA is still the law, and that despite some of what I heard, this rule does not require that you, for example, get all patients on the portal and push all their information to them immediately. But rather, if they, their representative or provider requests access, such as by signing up for and signing into the portal or using other electronic means to provide others access, then they have the right to that and they must have ongoing continuous access, exchange and use.

Slide 9

Definition: Actors

 **health care provider**

 health IT developer of certified health IT

 health information network or health information exchange (HIN or HIE)



More information: Who are actors and how are they defined? [Review the Information Blocking Actors fact sheet](#). Who is a health care provider? [Get details in the Health Care Provider Definition and Cross-Reference Table fact sheet](#).

So, let's discuss actors. For our purposes, healthcare providers are the primary topic here. If you're interested in going into detail about this, I encourage you to review the link resources on this slide, which the link was just chatted out as well. But the takeaway is that the vast majority of types of healthcare organizations and types of providers in those organizations are actors under healthcare providers, in this particular rule. Something to note here is that each of the three actors listed here on this slide are individually responsible for not blocking the exchange of EHI. Health IT developer or certified health IT is your EHR vendor and health IT vendors, you can look these up on the ONC website, there's a database where you can look up to see if your health IT or EHR vendor is certified health IT and therefore beholden to this rule as well.

Note that patients are not an actor, and are therefore not beholden to this rule. And therefore a patient can choose to share and not share information as they wish.

Slide 10

Definition: Electronic Health Information

Electronic Health Information for the purposes of information blocking, until October of 2022, is data elements represented in the [United States Core Data for Interoperability](#) (USCDI).

The Information Blocking final rule applies to all EHI and is not limited by when the information was created and pertains to all ePHI in a designated record set as defined by HIPAA, whether those records are used or maintained for or on behalf of a covered entity (again, information blocking rule pertains to all actors).

As of October of 2022, all actors will be required to make all EHI available for access, exchange, and use (no longer limited to elements in USCDI).

Review [FAQs](#) about Electronic Health Information answers on ONC's site.



Electronic health information or EHI, as we've mentioned already, until October of 2022, is limited to the data classes and elements in the United States Core Data for Interoperability, or USCDI, which we'll discuss in a moment. Note, one thing that's important to note is that EHR is not just limited to information created since the rule went into effect, but rather information that pertains to this in general.

Slide 11

USCDI

USCDI v1 Summary of Data Classes and Data Elements standards document, a brief summary of which is to the right.

Note that this list does not mean that you must have or collect all of this information, but rather that, basically, if it's in the electronic system [and thereby eHI], then it needs to be shared.

USCDI Data Classes		
Allergies and Intolerances	Health Concerns	Problems
Assessment and Plan of Treatment	Immunizations	Procedures
Care Team Member(s)	Laboratory	Provenance
Clinical Notes	Medications	Smoking Status
Unique Device Identifier(s) for a Patient's Implantable Device(s)	Patient Demographics	Goals

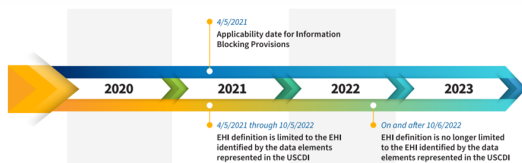
So as noted on the last slide, this rule currently applies to the USCDI. So what is the USCDI? It's the standardized set of health data classes in constituent data elements for nationwide interoperable health information exchange. USCDI version one includes 16 categories, including patient demographics, allergies and intolerance, smoking status, clinical notes, et cetera. Do note that clinical notes are included. But note that the following are not required to be shared.

Psychotherapy notes that are separated from the rest of an individual's medical record, and are recorded in any medium by healthcare provider who is a mental health professional documenting or analyzing a session. Note that all clinics and organizations are required to share other related information, meaning everything except the contents of the session. The organization open notes, which you may or may not be familiar with, has helpful information guidance and insight on the sharing of clinical notes, I recommend checking out their website.

Further, FAQs on ONC's page have several questions about EHI, many of which focus on the clinical notes portion. And then lastly, just note that this doesn't mean that you are required to collect all of this information, but rather that if you do have it and maintain it electronically, then it's subject to the information blocking rule.

Slide 12

Key Dates: Information Blocking



Source: Health Care Provider Definition and Cross-Reference Table, Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency Interim Final Rule

The takeaway on this slide is that after October of 2022, or about 14 months from now, the information blocking rule will no longer be just data defined by the USCDI, but all EHI.

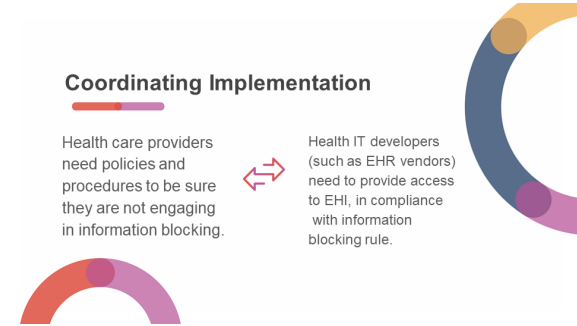
Slide 13

Coordinating Implementation

Health care providers need policies and procedures to be sure they are not engaging in information blocking.



Health IT developers (such as EHR vendors) need to provide access to EHI, in compliance with information blocking rule.



So let's move on to discussing some implementation considerations. As I mentioned earlier, actors are separately responsible for allowing access, exchange and use of data and not engaging in information blocking. This means that each type of actor is likely to rely on others not to block information. In practice, for example, a clinic needs to understand how their EHR is facilitating access and exchange of EHI, so that the clinic's policies can be based on that. And vice versa. Right? A health IT developer is relying on the clinics using software to configure and use it per the features in the software. So if you have an EHR, they've likely published some list or crosswalk of how the elements or data classes in the USCDI can be accessed, exchanged or used, and what is needed to do so.

And your compliance department or whoever handles this in your organization, which is likely to be someone in the larger organization, if you're part of a larger organization, has probably set forth some guidance for your clinics process for this, being sure that those two are aligned is really important for being able to actually implement successfully.

Slide 14

Eight Exceptions to Information Blocking Rule

Exceptions that involve not fulfilling requests to access, exchange, or use EHI

- Preventing Harm Exception
- Privacy Exception
- Security Exception
- Infeasibility Exception
- Health IT Performance Exception

Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI

- Content and Manner Exception
- Fees Exception
- Licensing Exception

For full details review the [Information Blocking Exceptions](#) fact sheet

I mentioned earlier that there are only eight exceptions to the information blocking rule, before I go through these, ONC's specifies that an actor's practice, meaning, for example, your clinic, that does not meet the conditions of an exception specified will not automatically constitute information blocking. Instead, such practices will be evaluated on a case by case basis to determine whether information blocking has occurred.

So let's talk about these exceptions. The five exceptions on the left side of the screen are those that actually permit not fulfilling a request, meaning not sharing certain information. Those on the right allow for flexibility or alternatives in how requests are handled, but still require sharing the information. So, blue box are those that allow not fulfilling your request, magenta box are those that allow some flexibility in how they're handled but still require sharing. Each of the eight exception types has specific conditions that need to be met in order for the exception to apply. Exceptions apply on a case by case

basis. I can't stress this enough. All of these have to be applied on a case by case basis, or all of the ones that we're going to talk about, and they are not broad based exceptions.

So for each instance, an exception could be applicable, but each instance needs to be individually addressed and any exceptions documented. There's too much here to cover in great detail today. We have chatted out the link to the details about the exceptions, and we're going to go deeper on three of them, preventing harm, privacy, and content and manner.

Slide 15

Preventing Harm Exception

- **Objective:** This exception recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of EHI.
- **Key Conditions of the Exception:**
 - The actor must hold a reasonable belief that the practice will substantially reduce a risk of harm
 - The actor's practice must be no broader than necessary
 - The actor's practice must satisfy at least one condition from each of the following categories: type of risk, type of harm, and implementation basis; and
 - The practice must satisfy the condition concerning a patient right to request review of an individualized determination of risk of harm.



For full details review the [Information Blocking Exceptions](#) fact sheet

First up is the preventing harm exception. According to ONC, this exception recognizes that the public interest ... sorry, recognizes the public interest in protecting patients and other persons against unreasonable risks of harm that can justify practices that are likely to interfere with access, exchange or use of EHI.

In short, organizations can deny EHI requests to protect patients or other consumers from harm. However, the potential risk and harm that would trigger the exception must be appropriately documented. Some questions to consider include, is the organization meaning your agency, able to segment sensitive health records of minors as protected by state and federal regulations so that parents don't have access to that information that they're not authorized to receive. And other question is, is the data complete and uncorrupted? The preventing harm exception says that it will not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person provided certain conditions are met.

In the FAQs, ONC has advised that in most instances, including where practice interferes with the patient's own or the patient's other health care providers legally permissible access, exchange or use of the patient's electronic health information, coverage under the preventing harm exception requires that the risk of harm be physical harm. So again, what this is saying is that in most instances, it requires that it be risk of physical harm, though the type of harm can be more broad in some limited circumstances. Specifically, the type of harm that must be present is one that's reasonably likely to endanger the life or physical safety of the individual or another person.

Further, ONC specifically tracks the same type of harm that is required to deny an individual access under HIPAA. So note that in the information blocking rule, the risk of such harm may be determined either by a licensed health care professional same as HIPAA, or arise from data that is known or reasonably suspected to be misidentified, mismatched, corrupted due to technical failure, or erroneous for another reason. Meaning that if data is known to be missing, corrupted or incorrectly matched, and as such could result in inappropriate care that could result in physical harm, for example, this exception could be applied.

And other note is that ONC states in the FAQs, that the preventing harm exception cannot be used to create a blanket delay in releasing lab or other test results by the ordering clinician, or so that the ordering clinician can evaluate the results prior to them going to the patient. It can be done on an individual case by case basis, but needs to be documented. So that was one of the questions that came in in the registration is, can we have a blanket delay in releasing lab or other test results to the portal, for example, such as a three to five day delay? And the answer is that, no, that can't be done, as a blanket delay, it needs to be done on an individual case by case basis, and we'll mention this again in a moment. But that is an example from the information blocking FAQs on ONC's site.

Slide 16

Privacy Exception

- **Objective:** This exception recognizes that if an actor is permitted to provide access, exchange, or use of EHI under a privacy law, then they should do so. However, an actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws.
- **Key Conditions of the Exception:** (must meet at least one of these 4 sub-exceptions)
 - Precondition not satisfied
 - Health IT developer of certified health IT not covered by HIPAA
 - Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a) (1) and (2)
 - **Respecting an individual's request not to share information:** An actor may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual, provided certain conditions are met.



For full details review the [Information Blocking Exceptions](#) fact sheet

The privacy exception, so now we're talking about the privacy exemption, and the privacy exception says that it will not be information blocking if an actor does not fulfill request to access, exchange or use EHI in order to protect an individual's privacy provided certain conditions are met. These conditions include, first, if an actor is required by state or federal law to satisfy a precondition, such as patient consent or authorization prior to providing access, exchange or use of EHI. The actor may choose not to provide access, exchange or use of such EHI if the precondition has not been satisfied under certain circumstances.

The second example is denial of an individual's request for their EHI consistent with what we discussed earlier, psychotherapy notes and information compiled in reasonable anticipation of civil criminal or administrative action. Those are not required to be shared, and it's this exception that would apply in that situation. Then third is respecting an individual's request to not share information. An actor may choose not to provide access, exchange or use of an individual's EHI if doing so fulfills the wishes of the individual provided certain conditions are met. So, this is really the key part of the privacy exception as we think about how to respect the wishes of an individual. In particular, when that individual has the right to request that their information not be shared.

So, under the privacy exemption, if an individual requests that their information not be shared, then the actor can choose not to share it. I see some questions in the chat. We will address those questions or questions along those lines in the Q&A portion. So thanks for sending those in.

Content and Manner Exception

- **Objective:** Provides clarity, flexibility to actors concerning the required content of an actor's response to a request to access, exchange, or use EHI and the manner in which the actor may fulfill the request. This exception supports innovation/ competition by allowing actors to first attempt to reach and maintain market negotiated terms for the access, exchange, and use of EHI.
- **Key Conditions of the Exception:**
 - **Content Condition:** Establishes the content an actor must provide in response to a request to access, exchange, or use EHI in order to satisfy the exception.
 - **Manner Condition:** Establishes the manner in which an actor must fulfill a request to access, exchange, or use EHI in order to satisfy this exception.



For full details review the [Information Blocking Exceptions](#) fact sheet

The third exception we're going to talk about is the content and manner exception. This exception specifies that it will not be information blocking for an actor to limit the content of its response to a request to access, exchange or use EHI, or the manner in which it fulfills the request to access, exchange or use EHI, provided certain conditions are met. This is one of the exceptions that relates to procedures for fulfilling requests for access, but does not allow for not filling requests.

So the last two refer to instances where it's okay to not fill requests provided it's documented. This is where we refer to procedures for fulfilling requests. ONC in their FAQ responses, notes that the content and manner exception does not require the use of any specific standard or functionality. Instead, the content and manner exception outlines a process by which an actor may prioritize the use of standards in fulfilling a request for EHI in a manner that supports and prioritizes the interoperability of the data. This means that for the purposes of information blocking, before October of 2022, and after May fulfill a request with EHI identified by the data elements represented in the USCDI standard, first, in the manner requested and if not, then in an alternate manner agreed upon with the requester following the order of priority specified.

So to summarize what this means, this exception may be the one that allows or supports a fairly standardized process, prioritizing standard based access, exchange and use. I believe that the idea here is that this will make it less of a free for all in terms of needing to provide any in all information and any in all forms requested. This is likely also an exception that comes into play if your health IT system or your EHR currently only provides access, exchange or use in a limited number of ways, it may be appropriate to rely on the manner condition of this exception, again offering the standards based manner of exchange first, such as patient portal or information exchange built into the EHR.

So, to draw that out a little further into what some may be experiencing. If the health IT system is not capable of access information ... sorry, access, exchange and use of information, then one of the earlier exceptions may apply, such as the health IT performance exception, until such time that health IT can be upgraded, though that can be no longer than is necessary. If the system can provide the EHI just not in the manner that the patient or patient's other provider requested it, then the content and manner exception may apply, in which case, the clinic would provide the information in the manner that's possible, which is what might be spelled out by the vendor, and you'll want to review the manner condition on page four of the exception document we chatted out earlier for more detail.

In all instances, where a request for EHI cannot be fulfilled in compliance with the information blocking rule then the clinic needs to document the exception and still needs to respond to the patient or the patient's provider with what is feasible.

Slide 18

Let's Look at Specific Examples



So let's look at some specific examples.

Slide 19

It *could be* information blocking to not provide access to...



...patients who seek to access their own EHI (including via third party).

...other providers who seek EHI for treatment or quality improvement.

...payers who seek EHI to confirm a clinical value.

...access to EHI for patient safety and public health.

One question that came in from registration for this webinar is, "Does delaying lab results to a patient via a portal for a set number of days or time constitute blocking?" The short answer to that is that a blanket delay on releasing lab results to a portal could constitute information blocking. Yes.

Delays can potentially be implemented on a case by case basis, such as for certain results for certain patients, but that needs to be documented on a case by case basis. There's several other options or possibilities that might be blocking on the screen, the key here is to be sure that you have policies and procedures in place that provide access or share information, and that any situation where that's not occurring or requests are not being fulfilled, are documented with the appropriate exception. And again, ONC says nothing is definitely information blocking. So, I really want to stress that, nothing is definitely information blocking. Having policies and procedures in place is important, making that good faith effort is really, really important.

ONC says nothing is definitely information blocking but rather that any complaint of information blocking would be reviewed on a case by case basis.

Slide 20

New Consideration: Third Party Apps



To learn more about this, review [There's an API for That](#)

Something new to consider is that patients are permitted to request that actions, make their actors, make their health information available to third party apps that's better designated by the patient themselves. So this would need to be designated by the patient themselves. They're certainly concerned that these apps may not be secure, or that they could compromise the confidentiality of health information.

In the 2020 rule, ONC makes it clear that a medical provider or a health care provider can educate the patient and warn them about the potential dangers associated with releasing their information to a third party app, but they can't prevent the data from being accessed by the app if requested by the patient. If this were to come up, it would be facilitated through your EHR using an API or something similar.

Slide 21

Adolescent Privacy

- The federal information sharing rules defer to state adolescent privacy and data sharing laws, which vary across the country.
- Availability of EHR features to facilitate needed segmentation of the data vary widely.
 - As such, systems are needed to facilitate parent/ guardian/proxy access to adolescent's health information where required, while protecting portions that a patient requests not be shared, where allowable by law.



[Read more from AAP in their preprint journal article.](#)

Another example probably of interest to this group is adolescent privacy. One of the keys to note here is that policies within your agency that broadly apply to all adolescents will not work, such as saying we consider all information or results for patients aged 12 to 16 sensitive and therefore we will not share them. As I mentioned earlier, blanket policies are generally not allowable, and rather need to be applied on a case by case basis. Each state has rules or regulations as to which health decisions a minor can make on their own, which come into play here.

Applying those on a case by case basis, typically require segmenting data in the EHR. So the thing to note here, to thread this needle is that processes and systems are needed to facilitate parent guardian proxy access to adolescent health information where required, while protecting the portions that a patient requests not be shared, where allowable by law. And remember that all of this, again, information blocking rules do not supersede state or local laws, rather, they go together. So it's where these things are allowable by law.

Slide 22

We don't use Certified EHR Technology (CEHRT), does this still apply to us?

According to [Information Blocking FAQs](#) on ONC's site, **yes**, any individual or entity that meets the definition of *at least one category* of actor—health care provider, health IT developer of certified health IT, or health information network or health information exchange—as defined in [45 CFR 171.102](#) is subject to the information blocking. The information blocking regulations apply to a health care provider, as defined in the Public Health Service Act and incorporated in 45 CFR 171.102, **regardless of whether any of the health IT the provider uses is certified under the ONC Health IT Certification Program.**

For full details review the [Information Blocking Actors](#) fact sheet

This goes back to what I've mentioned previously, each type of actor is individually responsible for not blocking EHI. So if you don't have a certified EHR, then there is not that additional actor in the mix, meaning that that second type of actor isn't in the mix. But healthcare providers are still an actor, even if they don't use certified health IT. So, ONC has said they are still beholden to this rule.

So someone in the registration questions asked, "If we're a small practice, and we don't have a patient portal, does this still apply to us?"

So, if you maintain health information electronically, this does still apply to you, regardless of whether you have a portal or not, regardless of whether you're using certified health IT or not. If you're maintaining information that meets the definition of EHI, then this does still apply to you.

Slide 23

How can you be ready?



So how can you be ready?

Slide 24

Review Your Current Processes

Review **existing policies and procedures** for receiving, processing, and responding to requests to access, exchange, or use EHI. Be sure to review any **fees charged to patients**.



Work with your EHR and other health IT vendors to **understand, identify, and implement policies or solutions** to support patient EHI access requests and comply with information blocking requirements.



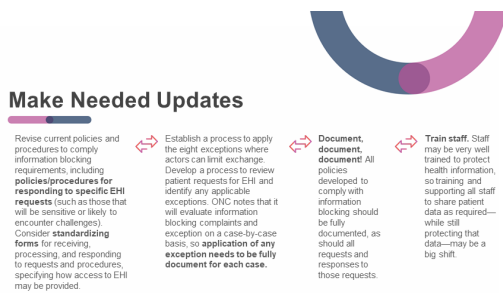
Evaluate **data use, business associate, and other agreements** that could intersect with information blocking, which may include agreements with health IT vendors, HIEs, hospitals, and other entities. Be sure these **comply with information blocking**, and include approaches to ensure access and exchange of EHI.

Read more from MGMA's [Information Blocking Toolkit for Medical Groups](#), from which the above is excerpted.

So first, review your current processes, you'll want to review your existing policies and procedures for receiving processing and responding to a request to access, exchange or use EHI. Be sure to review any fees charged to patients because that's part of this rule as well. There can't be excessive fees.

Work with your EHR and other health IT vendors to understand, identify and implement policies or solutions to support patient EHI access requests and comply with information blocking requirements. Next, you want to evaluate data use, business associate and other agreements that could intersect with information blocking, which may include agreements with health IT vendors, HIEs, hospitals, and other entities. So essentially, if you exchange information with other entities, it's important to ensure that these comply with information blocking, including approaches to ensure access and exchange of EHI.

Slide 25



And then make the needed updates. That's the next step. That includes revising term policies and procedures to comply with information blocking, including policies and procedures for responding to specific EHI requests, including those that are likely to be sensitive or likely to encounter challenges. Consider standardizing forms, an example of a standardized form that might be appropriate would be a request form that patients who do not want their information shared might complete and making sure that that form is used for the privacy exception if that's what you're going to do.

Establish your process to apply the eight exceptions where actors can limit exchange, and develop a process to review patient requests for EHI and identify any applicable exceptions. ONC notes that it will evaluate information blocking complaints and exceptions on a case by case basis. So again, I've said this many times, but just note that the key here is to document that on a case by case basis. Then it will be very important to document this as you go into train staff, staff may be very, very well trained to protect health information, we all know how important that is. So training and supporting all staff to share patient data as required while still protecting that data may be a big shift.

Slide 26

How can this benefit you?

So how can this benefit you? So somebody just asked in the chat, "How can we access MGMA's information blocking toolkit for medical groups?" It's linked in the slides, and Molly noted that a recording of today's webinar, the slide deck, and a transcript will be on RHNTC.org and shared with attendees in the next few days. So you'll be able to access it from that link there. So how does this benefit you?

Slide 27

You Can Access EHI from Others!

- Information Blocking rule doesn't just require that you provide access to others.
- It also requires that others provide access to EHI to you!
- All actors, including those you might be seeking to get results or records from, are not permitted to block access to EHI. The following are examples of what are may be information blocking:
 - Organizational policies or contract terms that prevent sharing information with patients or health care providers.
 - Technology is designed or implemented in non-standard ways that inhibit the exchange of information.
 - Patients or health care providers become "locked in" to a specific technology (such as an EHR) or health care network because data are not portable.



Examples provided are from the American Medical Association's [PART 1: What is information blocking?](#)

The rule not only allows patients and their representative to access and use information from you, but also you from them. So if you're currently receiving results by fax, or having to navigate some paper based system to get results or some other information, then this rule can support you in getting electronic access to the information.

You can be on the other end of this as well, and I think it's really important to know that we've heard from a lot of folks. So I saw somebody in the chat asks about how this intersects with F Part 2.0. One of the things that could potentially be the case is that if you are working with a client, and you want their results for any particular test, whether it be an STI test, or something like that, and they said they got it elsewhere, with their permission, you can request that information from that other provider and you and have that information in your system now, which helps you have that more complete F Part 2.0 data, for example. That's just one example.

Slide 28

Q&A

Addressing your questions
with Abigail English, JD



So let's move on to Q&A. I'm going to ask Abigail to join me.

We're going to get started, as I mentioned with the questions that you all posed. They're great questions that you've asked, and I will be posing your questions to Abigail. So to start, Abigail, how is a minor's consent affected by the information blocking rule?

Abigail English: Well, first of all, thank you, Jillian, for that question, and thank you also for including at the beginning of the webinar, a disclaimer that any information we provide is exactly that. It's information, and it's not legal advice, and I'll probably say this several times, just as you said, document, document, document, and decide things on a case by case basis several times. So it's very important for programs to consult with their legal counsel about these difficult questions, because as you said, a lot of these issues are very new. They're subject to ongoing evolution and clarification. And so, it's going to be really important for all of us to keep up, which is not easy to do, but is really important.

So, your question is, "How is the minor's consent affected by the information blocking rule?" I think it's really important for people to understand that the information blocking rule does not change the laws regarding when minors are allowed to consent for their own care. However, the rule may affect the confidentiality of information when minors are allowed to consent. Generally, state law determines when a minor is allowed to consent for their own care, and state laws allow some minors to consent based on their status, based on who they are, for example, if they are married, or if they are living apart from their parents or if they have reached a specific age.

State laws also allow minors to consent based on the services they are seeking. For example, for contraception, STI diagnosis and treatment, outpatient mental health care or substance use counseling and treatment. In addition, and particularly important for folks on today's webinar, in Title X funded sites, due to the strong Title X confidentiality regulations and the way they have been interpreted by the courts, minors can receive family planning services, and Title X funded sites without parental consent, and based on their own consent. This is not changed in any way by the information blocking rule.

At the same time, in Title X funded sites, when a minor receives family planning services, information about the services is confidential, except it can be disclosed with the minor's permission, or as required by law. Examples of laws that may require disclosure without the minor's permission include things like state child abuse reporting laws, and also potentially the information blocking rule. This is a little tricky because of what you described earlier, with respect to the privacy exception, and we'll get into that in a little bit. But the information blocking rule in some summation does not change the underlying law on minors consent, but may affect the ways in which confidential information about the minor's care is handled.

Jillian: Great, thank you. Just to draw that out to the next step, do any of our patient education or consent forms need to be modified based on these regulations?

Abigail: So, modification of the forms may or may not be necessary, however, it's likely that they will be, and it will be very important to review patient education and consent forms to determine whether any of the information contained in those forms needs to be changed as a result of the new requirements associated with the information blocking rule. So for example, if there is any information in those forms, or particularly in the patient education materials about what happens to information in the portal, who can sign up for the portal, who has access to the portal, what information will be made available through the portal, all of that needs to be carefully reviewed to be sure that the policies of the program or the site are consistent with the information blocking rule.

And also, as you mentioned earlier on, it may be necessary to create some new forms. So for example, to create a specific form that a minor could sign or that any patient could sign requesting that their information not be shared, or that certain aspects of their information not be shared, they might say it's fine to share information about vaccinations that I received, but not about STI tests that I've had. So,

being very specific in those forms are giving an opportunity for patients to be very specific in those forms, may be important. So I would say given the complexity and the broad reach of the information blocking rule, a really thorough review of all patient education materials, and all forms be undertaken and be left as they are, and some will need to be modified, probably, most likely.

Jillian: Got it. What I'm hearing is that we want to be sure that we're not promising patients, we are not going to share their information, when this rule may say there are instances where their information would be shared unless otherwise blocked or requested not to be shared. So we don't want to be making promises we can't keep.

Abigail: Exactly. Exactly.

Jillian: Got it.

Abigail: That's been a long standing issue, particularly in adolescent care because ... and I'm not speaking now specifically about Title X sites, but just in general, that often providers say things like, in a very well intentioned way, "Everything you told me will be confidential." But when in fact, confidentiality is never absolute. It's always subject to exceptions. It's been subject to exceptions prior to the information blocking rule, when a patient is presenting a serious risk of harm to themselves or others, or when they are suspected to be victims of child abuse or other forms of reportable abuse, that information has to be disclosed.

Jillian: That's a very good point.

Abigail: From an ethical perspective, it's always important to make clear to patients what the limitations are on confidentiality. But now with the information blocking rule, it's also very important from a legal perspective to make clear what might be required to be disclosed subject to the exceptions in the rule.

Jillian: Got it. The next question is, in your opinion, what needs to be considered when determining how to ensure minors or adolescent patients have access to the chart while maintaining confidentiality?

Abigail: So, if a Title X grantee or clinic has a web portal, and many of course do, it will be important to consider who would have access to the information in the portal, and to remind patients that anyone who has their password might be able to access their confidential information. Often, adolescent patient's parents know their passwords for various reasons. And if that is the case, a parent would be able to access the information in the patient's account in the portal.

In the past, providers who take care of adolescents have adopted a wide variety of approaches to ensure that adolescent's sensitive information that the adolescent wants to remain confidential is not disclosed to the parent without their permission, from halting access to the portal entirely between ages 12 or 13, and 17. Continuing to allow adolescence but not parents to access the portal, or creating hybrid approaches with parents having access to non sensitive information. These practices raise one of the questions that you addressed earlier in your presentation, which is that blanket rules generally are not going to fly under the ONC information blocking rule.

That in general sort of blanket on rules saying we're not going to disclose any of this is probably going to be problematic. So, in light of the information blocking rule, really all of these approaches need to be reviewed to determine whether they have been or can be structured in a way that complies with the rule, or whether they need to be converted into a different kind of system that is more case by case

where individualized determinations are made by the provider about what can and can't be withheld from disclosure, and often that may be as a result of the patient themselves requesting that certain information not be shared under the privacy exception. But again, that needs to be implemented on a case by case determination or basis.

One of the things that is definitely evolving, and I'm not either an EHR vendor or an IT expert, but the capacity of different EHR is to do different things and the capacity to create more automated ways to record the individualized determinations that providers have made, is evolving and, and because otherwise it could be very time consuming and burdensome for the provider to document what's necessary and that's why it's important that these evolutions are taking place in EHRs. The past practices ... and I'll just say a couple more things about this, the past practices were created in part to comply with confidentiality requirements in state minor consent laws and the HIPAA Privacy Rule.

The HIPAA Privacy Rule provides that when a minor can consent to their own care, their parents are not automatically their authorized representative with an automatic right of access to their information. So in light of this, one critical factor is segmentation in order to comply with the information blocking ban while also enabling compliance with state and federal health products laws, it's essential for providers to have the ability to segment information in a way that access, exchange and use are facilitated for shareable information, and sensitive information is protected from inappropriate sharing.

The preventing harm exception, as you mentioned, is also a critical one to consider. If releasing information to a portal that a parent might have access to, could potentially cause harm to the patient, the provider needs to consider, again, whether their EHR has the capacity to segment the information or otherwise protected from inappropriate release. With respect to each of these considerations, it's essential to consult with legal counsel to be sure that all conditions are met for any exception that's being relied on and with IT experts to determine what is feasible in the EHR.

Jillian: Perfect, thank you. So, a couple of questions have come in. Is there a difference in different types of visits? For example, does information blocking apply differently in visits where a patient is under age 18, or telehealth visits?

Abigail: The information blocking rules requirement to avoid interference with access, exchange and use of EHI focuses on the specific types of actors in the case of today's webinar, healthcare providers, and on the specific categories of EHI that are covered by the ban. So there's no overall exclusion of particular types of visits such as visits with patients under age 18, or telehealth visits. Information from adolescent visits and or telehealth visits are included within the data sets to which the information blocking ban applies.

However, some EHIs have created mechanisms whereby adolescent visits can be designated as confidential visits, or notes from those visits can be designated as confidential notes, which may affect whether and how information about those visits or notes from the visits are transmitted to the portal, or are provided in response to records requests. This terrain is evolving quickly with new explanation or interpretations of the rule. So it is not entirely clear at this moment, the extent to which these different mechanisms developed in the past, will be considered consistent with the information blocking rule compliance. Again, consultation with legal counsel and IT experts is essential.

Jillian: Absolutely. Just to draw that out a little bit further, someone noted that their family planning practices use a confidential visit for all minors, that allows the information to be blocked from sharing

with the HIE to keep their family planning information confidential. Would that work? Would a similar approach work here?

Abigail: I would really need to think about that a little bit more. I hate to give-

Jillian: That's fine.

Abigail: ... across the board answer. I think there may be a way that it could be structured to work, and it might require some more individualized mechanisms involving individualized requests from patients or individualized determinations by clinicians. I don't really think I can give an across the board answer to that one.

Jillian: No problem. The summary that I would give is that if that's what you're doing, the important part is to assess whether that is addressing these individual requirements, these case by case requirements that are required for information blocking currently.

All right, great. I believe I accidentally skipped a question, I'm going to go back to that one, which is to say that at least one agency is concerned about maintaining adolescent patient confidentiality, and parent satisfaction in a manner that allows the patient to pursue continuity. What would you advise this agency to consider?

Abigail: I would say one option can always be to explore the extent to which patients are willing to share some or all information with their parents. Research has shown that a majority of adolescents do share information about their care even when they're seeking family planning services. If minors are unwilling to share all of their information but willing to share some, then the capacity to segment information, the EHR, again, becomes critical.

As mentioned previously, the capacity of different EHR systems to facilitate the level of granular segmentation needed to protect sensitive information while facilitating appropriate sharing is definitely evolving. But the privacy exception to the information blocking ban does allow a provider not to share information if the patient has requested that. So, two primary considerations in these circumstances would be adolescent patient willingness to share information and the EHR capacity to segment information.

Another important consideration would be whether there is a way to create patient education materials that can be shared with parents, but explain any limitations on access to information in a way that's generalized rather than specific to individual patients in order to avoid parents being dissatisfied when and if they are unable to access certain information.

Jillian: That's a great point. Many great points there, and I feel like we hadn't touched on any of them. I think that is mostly a perfect place to stop. I'm going to move us forward. Thank you, Abigail, for sharing that information in response to these questions, and thanks for those who submitted questions.

Slide 29



How to Engage with Us



Subscribe to the RHNTC monthly eNewsletter at rhntc.org/enewsletter



Contact us on rhntc.org



Sign up for an account on rhntc.org



Follow us on Twitter @[rh_ntc](https://twitter.com/rh_ntc)

Just a reminder that there's a number of ways that you can engage with us, you can subscribe to the newsletter, you can contact us on rhntc.org, follow us on Twitter. Lastly, I just want to say thank you all for joining us today, and I hope you'll join me in thanking Abigail for joining us as well.

As a reminder, we'll have materials from today's session available in the next few days. If you have additional questions for the RHNTC on this topic, don't hesitate to email us at rhntc@jsi.com.

Slide 30



rhntc.org

THANK YOU!

Visit RHNTC.org or contact us at rhntc@jsi.com!

Please fill out the evaluation form after the webinar!

This webinar was supported by the Office of Population Affairs (Grants PFFPA000030, TFGA4000006) and the Office on Women's Health (Grant A57W40000-30-01-00). The views expressed do not necessarily reflect the official policies of the Department of Health and Human Services, nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Our final ask is that you please complete the evaluation today. The link to the evaluation will appear when you leave the webinar and will also be emailed to you after the webinar. We really love getting your feedback and we use it to inform future sessions. Thank you again for joining us. This concludes today's webinar.