Information Blocking and Exceptions to Sharing EHI

Denise Webb, Health IT Executive Advisor, Pivot Point Consulting

January 12, 2022

Disclaimers

- This presentation is for informational purposes only
- It does NOT, and is not intended to, constitute legal advice
- Only your attorney can provide assurances regarding the application of this information to your particular circumstances
- The statements, views and opinions expressed in this presentation are solely those of the presenter, and not those of CHCANYS
- The statements, views and opinions expressed in this presentation are solely those of the presenter, and not those of the ONC

Thank you for joining us today.
This is intended to teach and provide you with the information to have an informed discussion regarding how to address and meet the requirements of the information blocking provision and exceptions in your organization.

About the Empowering Patients Educational Series

- Designed to support CHCANYS members as they work toward compliance with information blocking regulations stemming from the 21st Century Cures Act
- November 2021-March 2022
- Includes:
  - Webinar presentations providing foundational knowledge for all member roles (provider, compliance, HIM)
  - Ask the Experts interactive Q&A sessions focusing on information needs of specific member roles
  - Supporting resources to help members operationalize the regulations within their organizations

Note that we've included a calendar slide at the end
Not only roles but use cases as well
Will be providing the recording and slides after the presentation

Agenda

- Learning Objectives
- Legal Basis for Information Blocking Provision
- Key Terms and Definitions
- Information Blocking Exceptions
- Consumer Third-Party Applications
- Information Blocking Enforcement
- Q&A

Today's Learning Objectives

- Understand the legal basis for the information blocking provision and key terms
- Understand the eight information blocking exceptions and their purpose
- Know the conditions providers are required to meet to qualify for an exception to sharing health information and avoid claims of information blocking by requestors of EHI
- Recognize how the exceptions impact your organization, roles, and workflows
- Determine when it may be appropriate to engage legal counsel in interpreting and applying the exceptions
- Understand the information blocking enforcement authority and provisions of the Cures Act

Legal Basis for Information Blocking Provision

- 21st Century Cures Act, Section 4004
  - Defines Information Blocking
  - Authorizes the Secretary of HHS through notice and comment rulemaking to identify reasonable and necessary activities that do not constitute information blocking

The 21st Century Cures Act provides the legal basis for the Information Blocking provision and requirements in the ONC rule. The Act defined information blocking and authorized the HHS secretary to identify reasonable and necessary activities that do not constitute information blocking. The ONC's Final Rule on Interoperability, Information Blocking, and Health IT Certification Program addresses these activities as exceptions and provides for eight exceptions to information sharing that would not be considered information blocking.

The information blocking provision was enacted in response to concerns that some individuals and entities are engaging in practices that unreasonably limit the availability and use
of electronic health information (EHI) for authorized and permitted purposes. These practices undermine public and private sector investments in the nation's health IT infrastructure and
frustrate efforts to use modern technologies to improve health care quality and efficiency, accelerate research and innovation, and provide greater value and choice to health care Consumers.

The primary objective of the information blocking provision is promoting interoperability and sharing health information with patients and their providers electronically though standards-based access, exchange, and use. The information blocking provision is focused on enabling electronic information sharing and providing necessary and reasonable exceptions to when it is ok to delay sharing or

not share electronic health information. ONC has shifted its messaging away from the term information blocking exceptions to information sharing exceptions.

CMS's final rule on interoperability and patient access had some information blocking provisions related to the Promoting Interoperability Program which is separate and distinct from the ONC information blocking provisions and enforcement. This webinar is specifically covering ONC's rule concerning information blocking.

Key Terms and Definitions

- Information Blocking
- Electronic Health Information (EHI)
- Actors
- Access, exchange, and use
- Interoperability elements

It is important to understand some of the key terms and definitions in context of the Information Blocking provision before covering the exceptions to information sharing. We will cover the terms listed here and address what information blocking is, what information does information blocking apply to, who does it apply to, and when and how does it apply. Additional terms are defined in a glossary slides at the end of the deck.

Key Terms and Definitions: Information Blocking

A practice that is:

(1) Likely to interfere with the access, exchange, and use of electronic health information (EHI) except as required by law or covered by an exception; and

(2) Conducted by a health care provider that knows that such practice is unreasonable and likely to interfere with access, exchange, or use of EHI.

Some examples that would likely meet the definition of information blocking.

Restrictions on access, exchange, and use, such as may be expressed in contracts, license terms, EHI sharing policies, organizational policies or procedures could lead to an information blocking claim. For example, if a provider has provisions in their contracts or business associate agreements that prevent sharing of EHI that would otherwise be legally permissible to share, this is likely information blocking. In cases where the HIPAA privacy rule permits sharing of PHI, such as for treatment, payment and health care operations, the information blocking provision requires electronic PHI to be shared unless a law preempts sharing or the provider meets an exception.

If a provider limits or restricts the interoperability of health IT, such as disabling or restricting the use of a capability that enables sharing EHI with users of other systems or restricting access to EHI by certain types of persons or purposes that are legally permissible, or refusing to register a software application that enables patient access to their EHI assuming there is not a legitimate security reason that meets the conditions of the security exception.

If a provider takes several days to respond to a patient's request or an unaffiliated health care provider's request for a patient's EHI when they have the capability to provide same-day access to the EHI in the electronic form and format requested, this is likely information blocking.

Key Terms and Definitions: Electronic Health Information (EHI)

- Electronic protected health information (ePHI) in a designated record set
- Prior to October 6, 2022, EHI definition for the purposes of the information blocking is limited to the data elements represented in the US Core Data for Interoperability (USCDI) V1 standard

ONC's Cures Act Final Rule narrowed the proposed broader definition of EHI and aligned it with HIPAA definition of PHI and designated record set.

As defined in the HIPAA Rules, the designated record set comprises:

- medical records and billing records about individuals;
- enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan;
- other records used, in whole or in part, to make decisions about individuals.

The term "record" means any item, collection, or grouping of information that includes protected health information.

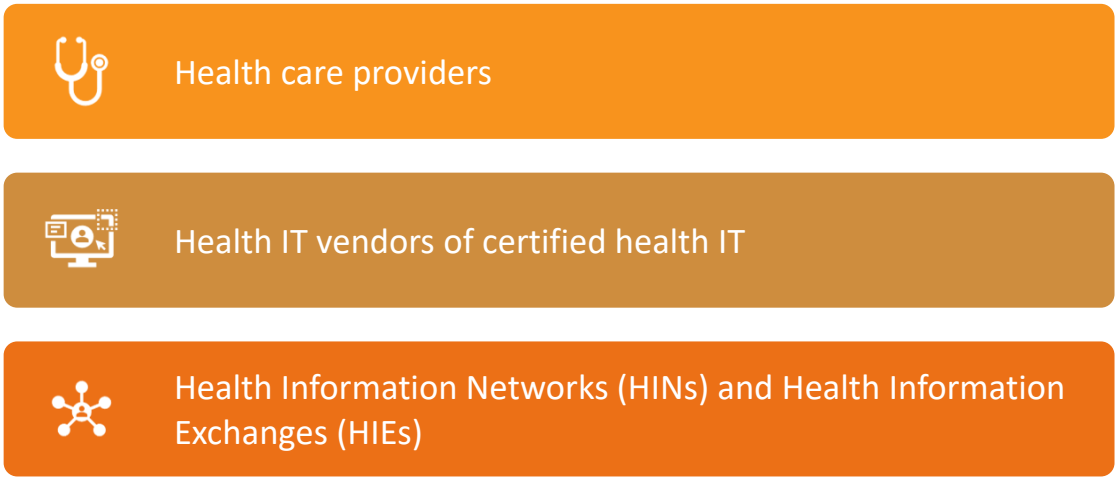
EHI does not include psychotherapy notes or information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding.

Health information that is deidentified consistent with the HIPAA regulations is NOT included in the EHI definition. Once PHI has been de-identified, it is no longer considered PHI.

ONC further narrowed the scope of EHI for the first 24 months after the Final Rule was published and confined EHI to the data elements in the US Core Data for Interoperability version 1. The ONC Interim Final Rule released last fall extended this narrower definition through October 5, 2022.

USCDI version 1 is the Clinical Common Data Set (CCDS) plus clinical notes, address, phone number, email address, provenance data, unique device identifiers for patient's implantable devices, and pediatric vital signs. Providers are not expected to share the EHI using the standards in the USCDI for each of the data elements if not technically capable of doing so. However, if your providers are participating in MACRA/MIPS, they must use an updated 2015 Edition of their EMR that meets the ONC 21st Century Cures Act Rule and ONC IFR certification standards beginning in 2023.

Key Terms and Definitions: Actors



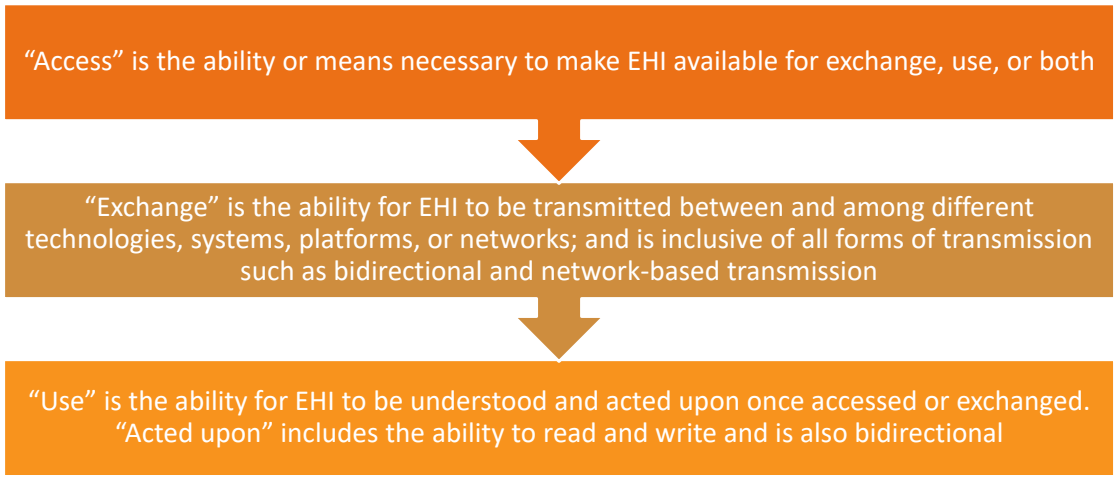
Health care provider definition is broad as defined in (Public Health and Welfare) 42 U.S.C. 300jj (3) and includes hospitals, skilled nursing facilities, nursing facilities, home health entities or other long term care facilities, health care clinics, community mental health centers, renal dialysis facilities, blood centers, ambulatory surgical centers, emergency medical services providers, federally qualified health centers, group practices, pharmacists, pharmacies, laboratories, physicians, advanced practitioners (physician assistant, nurse practitioner, clinical nurse specialist, certified registered nurse anesthetist, certified nurse-midwife, clinical social worker, clinical psychologist, and registered dietitian or nutrition professional), providers operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization, rural health clinics, covered entities under section 256b of this title, ambulatory surgical centers, therapists, and any other categories of health care facility, entity, practitioner, or clinician determined appropriate by the HHS Secretary.

Health IT vendors of certified Health IT – vendors that participate in the ONC Health IT Certification program.

HIN and HIE (May apply to health care provider)—Individual or entity that determines, controls, or has discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology for access, exchange, or use of EHI: (1) Among more than two unaffiliated individuals or entities (other than individual or entity to which this

definition might apply) that are enabled to exchange with each other; and (2) Is for a treatment, payment, or health care operations (TPO) purpose regardless of whether individuals or entities are subject to 45 CFR 160 and 164.

Key Terms and Definitions: Access, Exchange, and Use



The information blocking provision specifically addresses sharing electronic information via electronic methods and is focused on promoting health IT interoperability.

The definitions from the ONC rule provided on this slide illustrate what is meant by access, exchange, and use when it comes to the information blocking provision.

Providers must meet their HIPAA obligations when it comes release of information or a patient's individual right of access to his or her health care information. Providers still to fulfill requests for EHI, either on paper or on some other media, such as a CD or flash drive, if the provider can't fulfill an electronic request for access, exchange, or use of EHI through a network-based means.

Key Terms and Definitions: Interoperability Elements

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) Are controlled by the actor, including the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, and use of EHI.

Interoperability elements as defined here are the how of electronic access, exchange, and use of EHI and not providing the ability to use interoperability elements could be considered information blocking.

It is important for actors who control interoperability elements to understand that they are not required to license their IP for health IT that includes interoperability elements if needed to respond to a request for EHI in the manner requested as long as the actor can respond in an alternative manner or meet an exception. Generally, what a health care organization needs to understand with regards to interoperability elements is that if they for instance locally host and control a FHIR server for EHI access and exchange, rather than the vendor, they need to ensure that they are not configuring it in a way that prevents access, exchange and use of EHI. The same would apply to the configuration of interoperability elements within their certified health IT. If a provider is using proprietary APIs they don't control, this definition makes it clear the provider is not expected to infringe upon IP rights to fulfil a request for EHI that would require such infringement.

Health care CIOs should assess what interoperability elements, if any, they have under their control and review any policies or procedures they have in place regarding these interoperability elements to ensure alignment with the requirements of the information blocking provision.

Information Blocking Exceptions

"Required by Law"

Reasonable and necessary activities or "practices" identified as exceptions

- Preventing harm
- Privacy
- Security
- Health IT performance
- Infeasibility
- Content and manner
- Fees
- Licensing

If a provider interferes with or withholds access, exchange and use of EHI because is "required by law," then that practice would not meet the definition of information blocking.

Activities that are likely to interfere with access, exchange, and use but are reasonable and necessary practices are identified as exceptions to sharing or delaying the sharing of EHI in the information blocking provision.

The final rule clarified an actor must satisfy all applicable conditions of an exception at *all relevant times* to meet an exception. Each exception is limited to certain practices that clearly advance the aims of the information blocking provision and are tailored to align with the following criteria:

First, be reasonable and necessary: This includes practices that provide appropriate protections to prevent harm to patients and others; promote the privacy and security of EHI; promote competition and innovation in health IT and its use to provide health care services to consumers and develop an efficient means of health care delivery; and allow system downtime to implement upgrades, repairs, and other changes to health IT .
Next, each exception addresses a significant risk of actors choosing to not engage in beneficial and necessary practices because of the actor's uncertainty about the breadth and applicability of the information blocking provision.
Finally, each exception is subject to strict conditions to ensure practices are

limited to those that are reasonable and necessary.

The first five are exceptions that involve not fulfilling requests to access, exchange, or use EHI. The last three are exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI. Health care providers as HIPAA covered entities and their business associates will find they are already familiar with the conditions in the preventing harm, privacy, security exceptions which align with the HIPAA Privacy and Security rules that regulate the sharing and protection of PHI whether om paper or on electronic media.

It is important for your organizations to become familiar with these exceptions and know what is required to qualify for an exception to information blocking, so your organization can have an effective response should an information blocking complaint be filed against it and subsequently investigated by the HHS OIG. Your organizations will want to review its policies and practices to ensure alignment with these exceptions and make any needed adjustments.

The first three information blocking exceptions we will cover: “Preventing Harm,” “Privacy,” and “Security,” address reasonable and necessary practices that a provider organization conducts to address and manage patient safety, privacy, and security risks. These exceptions are structured to operate in a manner consistent with the framework of the HIPAA Privacy and Security Rules and to streamline your organization’s compliance with HIPAA and the ONC information blocking provision.

Any analysis of an information blocking claim will require consideration of the individual facts and circumstances, including whether the actions the practice or activity that interfered with access, exchange and use of EHI was required by law, whether the provider had requisite knowledge, and whether one or more exceptions apply. Failing to meet the conditions of an exception does not mean a practice is information blocking, only that it would not have guaranteed protection from penalties or disincentives and would be evaluated on case-by-case basis by the OIG for level of impact, intent, and knowledge.

Preventing Harm Exception

- Includes practices that are likely to interfere with the access, exchange, or use of EHI in order to prevent harm to a patient or another individual
- Practice must meet certain conditions:
  1. Reasonable belief practice will substantially reduce risk of harm
  2. Breadth of practice must be no broader than necessary
  3. And at least one condition from each of the following categories:
     A. Type of risk
     B. Type of harm
     C. Practice implemented based on a written organizational policy or a determination specific to facts and circumstances
  4. Fulfill patient's right to have individualized risk of harm determination reviewed and potentially reversed, if applicable

The Preventing Harm exception addresses practices related to patient safety that are likely to interfere or actually do interfere with the access, exchange, or use of EHI.

First, the provider must have a reasonable belief that their practice that is likely to or does interfere with access, exchange, and use of EHI will substantially reduce the risk of harm to the patient or another person that would otherwise arise from the access, exchange, or use of EHI.

Second, the practice taken must not be broader than needed to substantially reduce the risk of harm that the practice is implemented to reduce. For example, if only some EHI is affected and can be segmented, the remainder of the EHI should be provided. Another example is the scenario when a discovery of erroneous data is reasonably likely to endanger the life or physical safety of the patient. The practice implemented to substantially reduce risk is to delay access, exchange, or use to provide time to correct the data errors. This practice would qualify for this exception if the practice addresses the data issue and subsequently provides the access to the EHI, even though delayed.

Third, at least one condition for each of the following categories must be met:
<u>Type of Risk</u>
Risk must be at least one of two types: risk determined by licensed healthcare provider or a risk stemming form data issues

Type of Harm

There are four types of harm standards that apply and align with the harm standards that providers already have to comply with under HIPAA regarding release of paper records. See appendix for permissible, or details.

Org Policy or Determination specific to facts and circumstances

The practice must be consistent with a written organizational policy that is:

- Based on relevant clinical, technical, other appropriate expertise;
- Implemented in a consistent and non-discriminatory manner; and
- Conforms each practice to the conditions in the Risk of Harm exception that I covered above.

If a provider doesn't have an organizational policy such as may be the case for some solo or small practices that may not have comprehensive and formal policies, the practice must be based on a determination that relied on:

- Facts and circumstances known or reasonably believed at the time the determination is made and while the practice is in use; and
- Expertise relevant to implementing the practice consistent with the conditions in the Risk of Harm exception that I covered.

Even if an organizational policy exists, ONC understands it may be hard to anticipate all the potential risks of harm that could arise in real-world health IT clinical or production environments. Therefore, in these circumstances, the provider could justify the practice or practices based on the particular facts and circumstances to show the practice is necessary and no broader than necessary to mitigate the risk of harm.

Patient review rights condition

In the circumstances under the type of harm condition where a practice interferes with the access, exchange or use of a patient's EHI on the basis of a risk of harm determination by a health care professional, the provider must implement its practice in a way that allows for the patient whose EHI is affected to exercise his/her rights under HIPAA or any federal, state, or tribal law to have the individualized determination of risk of harm reviewed and potentially reversed.

Privacy Exception / Sub-Exceptions

- Addresses practices that are likely to interfere with the access, exchange, or use of EHI in order to protect a patient's privacy rights under HIPAA
- Four sub-exceptions available under certain conditions
  - Pre-condition not satisfied
  - Health IT developer of certified health IT not covered by HIPAA
  - Denying individual's right of access to EHI
  - Respecting individual's request not to share

The Privacy Exception is structured to operate in a manner consistent with the framework of the HIPAA Privacy Rules with which covered entities and their business associates are already familiar. ONC finalized the sub-exceptions to the Privacy Exception to ensure individual privacy rights are not diminished as a consequence of the information blocking provision and to ensure the information blocking provision does not require the use or disclosure of EHI in a way not permitted under the HIPAA Privacy Rule.

This exception is structured with four discrete "sub-exceptions." An actor's practice must qualify for a sub-exception and the conditions of the sub-exception to be covered by the Privacy Exception. The sub-exceptions have, to a large extent, been crafted to closely mirror privacy-protective practices presently recognized under federal and state privacy laws. See details of each in Appendix.

<u>Precondition not satisfied</u>
This sub-exception relates to federal or state law requiring a precondition be met before sharing the EHI. All conditions of this sub-exception outline in the Appendix must be satisfied.

<u>Heath IT developer of certified health IT not covered by HIPAA</u>
This sub-exception relates to when a health IT developer that is not a health care provider offers a certified consumer app to consumers directly. For example: a health IT developer creates and obtains ONC certification for a diabetes tracking

application and offers this app to consumer's directly, including certain privacy provisions in its offering. Developer is not subject to HIPAA but would meet the definition of an actor under the information blocking provisions because the product is certified health IT. See appendix for details on the conditions that must be met by the health IT developer to qualify for this Privacy sub-exception.

Denying individual's right of access to EHI

This sub-exception permits a covered entity or business associate to deny an individual's request for access to his or her EHI consistent with the HIPAA Privacy rule, such as psychotherapy notes or PHI created or obtained in course of research that includes treatment. See appendix for complete list of PHI that can be withheld under this sub-exception.

Respecting individual's request not to share:

Unless otherwise required by law, a provider can elect to not provide access, exchange, and use of an individual's EHI upon an individual's request and qualify for this sub-exception.

For the purposes of this exception only, the term "*individual"* encompasses any or all of the following:

- An individual as defined by the HIPAA Privacy Rule;
- A person who is the subject of EHI being accessed, exchanged, or used;
- A person who legally acts on behalf of the individual in making health care-related decisions as a personal representative as defined by the HIPAA Privacy Rule;
- A person who is a legal representative of and can make health care decisions on behalf of an individual; or
- An executor or administrator or other person having authority to act on behalf of a deceased person or the individual's estate under state or other law.

Security Exception

- Addresses practices that are likely to interfere with the access, exchange, or use of EHI in order to protect the security of EHI and mitigating risks to a provider's network and infrastructure
- The practice must be:
  - Directly related to safeguarding the confidentiality, integrity, and availability of EHI
  - Tailored to the specific security risk addressed
  - Implemented in a consistent and non-discriminatory manner
  - Implemented either in accordance with a written organizational policy or have a determination made in each case based on the particular facts and circumstances

The first condition under this exception is that the practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI. Substantiation of this condition being met by the provider includes but is not limited to the provider's basis for adopting a particular security practice evidenced by the provider's written organizational security policy, risk assessments the provider has performed that informed their security-based practice or practices, and other relevant documentation the provider maintains, such as documentation maintained as a part of its HIPAA security risk assessment and mitigation plans that supports meeting the HIPAA Security Rule.

The second condition is that the practice must be tailored to the specific security risk addressed. This condition presumes the provider evaluated the risks posed by the security threat and developed a response tailored to mitigate the health IT or other related system vulnerabilities.

The third condition is that the practice must be implemented in a consistent and non-discriminatory manner. This means the provider treats similarly situated actors whose interactions pose the same level of security risk consistently with one another under the provider's security policies.

The fourth condition requires a provider's practices that are likely to interfere with the access, exchange, or use of EHI be implemented in accordance with a written organizational security policy. The policy must:

1) Be based on and be directly responsive to security risks identified and assessed by or on behalf of the provider; align with one of more applicable consensus-based standards or best practice guidance; and
2) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.
In the case where a provider's security practice is not implementing a written organizational policy, the provider must have made a determination in each case based on the particular facts and circumstances that:
a) The practice is necessary to mitigate the security risk to EHI; and
b) There are no reasonable alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

Health IT Performance Exception

- Addresses practices implemented to maintain or improve health IT performance that are likely to interfere with the access, exchange, or use of EHI that meet certain conditions:
  - Maintenance and improvement of health IT
  - Assured level of performance and actions of third-party applications
  - Intersection with Preventing Harm and Security exceptions

The health IT performance exception addresses practices a health care provider or their health IT service providers, which include vendors of certified health IT or health information networks or exchanges, need to conduct to maintain the health and performance of their networks, infrastructure, and applications. Any outage or degradation would potentially impact the access, exchange, and use of some or all EHI and would not be considered information blocking if certain conditions and requirements of this exception are met.

Maintenance and improvements to the health IT must be the following conditions:
Implemented no longer than necessary,
Implemented in a consistent and non-discriminatory manner, and
Be consistent with service level agreements (SLAs) for planned or unplanned downtime or for unplanned downtime agreed to

The assured level of performance condition addresses situations where a third-party application is operating or behaving in a way that does not pose a security risk but is negatively impacting the performance of an actor's network, servers, or core functions of other applications.

The last condition of this exception addresses the intersection of health IT performance with the preventing harm and security exceptions. The health IT Performance exception expressly does not apply for maintenance and improvements aimed at preventing harm to a patient or other person, or to

security-related practices and instead the actor's practices would need to comply with the Preventing Harm and Security exceptions, respectively. For example, if an individual or an application is making or attempting unauthorized access to systems or EHI, the actor with control of the system subject to the security risk should take prompt action to address the risk which include health IT downtime or degradation. An example of this was the Wannacry malware that hit a number of hospital and health system networks a few years ago.

Infeasibility Exception

- Addresses practices of not fulfilling a request to access, exchange, or use EHI due to the infeasibility of the request under certain conditions
- To qualify for the infeasibility exception, one of the following conditions must apply:
  - Uncontrollable events beyond a provider's control
  - EHI segmentation
  - Request is infeasible under the circumstances

The first condition is uncontrollable events. These are events that are beyond a provider's control, such as a public health emergency, a natural disaster, or an internet service outage. A complete list of applicable events is provided in the Appendix. If any of the applicable events prevents a provider from providing access, exchange, or use of EHI, then that is all that is necessary to meet the infeasibility exception and no consideration of factors must be demonstrated or proven by the provider. An uptick in COVID-19 infections in your organization resulting in a shortage in staffing and Hurricane Katrina are examples.

The next condition is segmentation. This condition would apply in cases where the provider receives a request for access, exchange, or use of EHI, and the provider is required to withhold certain EHI, but the provider cannot unambiguously segment the EHI that has to be withheld from the EHI that is provided. The withholding of certain EHI could be due to a patient's preference, a law or to prevent harm in accordance with the Preventing Harm Exception.

The infeasibility under the circumstances condition is helpful to providers with limited technical capability to provide access, exchange, and use of EHI in a technical manner requested or an alternative technical manner. A provider who demonstrates prior to responding to the requestor that the request would be infeasible under the circumstances can qualify for the infeasibility exception. The rule requires the provider to do this through a written record or other documentation of its consideration of specified factors. See the appendix for the

additional requirements and specified determination factors that must be met to meet this condition.

Content and Manner Exception

- Addresses the practice of an actor limiting the content of its response to a request and the manner in which it fulfills a request to access, exchange, or use EHI
  - Content condition
  - Manner condition

The previous five exceptions addressed practices that are likely to or do interfere with access, exchange and use of EHI. The final three information blocking exceptions: Content and Manner, Fees, and Licensing involve procedures for fulfilling requests to access, exchange, or use electronic health information, and there are interdependencies among the three exceptions.

Content and Manner Exception

- Content condition
  - Scope of EHI provided until October 5, 2022
    - U.S. Core Data for Interoperability (USCDI) Ver 1 data elements

A USCDI "Data Class" is an aggregation of various Data Elements by a common theme or use case. Current classes include:

- Allergies and intolerances
- Assessment and Plan of Treatment
- Care Team Members
- Clinical Notes
- Patient Goals
- Health Concerns
- Immunizations
- Laboratory
- Medications
- Patient Demographics
- Problems
- Procedures
- Provenance
- Smoking Status
- Unique Device Identifiers
- Vital Signs

  - Scope of EHI provided after October 5, 2022 includes any/all EHI

The Content condition addresses the data a provider or other actor must provide electronically when requested. The scope of EHI providers are required to provide if requested up to and until October 5, 2022 are the data elements in the US Core Data for Interoperability version 1. After October 5, 2022, the scope is any EHI requested and is not limited to the USCDI data elements. Remember EHI is any electronic protected health information in a designated record set as defined in the HIPAA Privacy Rule.

The USCDI standard currently includes the data classes listed on the slide and within each data class there are one or more data elements. Version 1 includes all the data elements in the Clinical Common Data Set, plus some new data elements in patient demographics, provenance, unique device identifiers, and vital signs. Those providers who presently use a 2015 Edition certified EHR should have the technical capability to exchange the CCDS data elements now. Some vendors have already updated or are working on updating their health IT modules that are impacted by the USCDI standard. CIOs should follow up with their vendors on the availability of the updates. Hopefully, many vendors will be ready in advance of the December 31, 2022 deadline by which they must make these updates available, giving time for CIOs to implement the changes.

Content and Manner Exception

- **Manner condition**
  - Fulfill request in "any manner" requested if
    - Technically able and
    - Able to reach agreeable terms and conditions, such as technical, fees, licensing, etc.
      - Not required to satisfy requirements of fees and licensing exceptions
  - Or technically fulfill request in an "alternative manner" in the following priority order:

    1. Using technology certified to Part 170 adopted standard(s) specified by requestor

    2. Using content and transport standards specified by the requestor and published by the federal government or a standards developing organization accredited by the American National Standards Institute (ANSI)

    3. Using a mutually agreeable alternative machine-readable format, including the means to interpret the EHI

    AND any fees or licensing terms must comply with the requirements of the Fees and Licensing exceptions
  - If burden of fulfilling a request in "any manner" or an "alternative manner" specified is significant, then the Infeasibility exception may apply

If the burden on the actor for fulfilling a request is so significant that the actor chooses to not fulfill the request at all, the actor could seek coverage under the Infeasibility Exception.

Fees Exception

- Addresses actor's practice of charging fees for accessing, exchanging, or using EHI and conditions that must be met:
  - Basis of fees condition
  - Excluded fees condition
  - Compliance with the Conditions of Certification condition
    - Only applicable to health IT developers of certified health IT

The Fees exception has three conditions. To qualify for this exception, the actor's practice for charging fees to provide access, exchange, or use of EHI must meet the *"Basis of fees condition,"* and not include any of the fees addressed in the *"Excluded fees condition."* The details of the Basis of fees and Excluded fees conditions are provided in the Appendix. Also if the actor is a health IT developer of certified health IT subject to the Conditions of Certification, this actor must also comply with the *"Compliance with the Conditions of Certification condition*." The requirements of this exception do not apply if an actor fulfills a request for EHI in the "any manner" requested that requires a work effort on the part of the actor and the requestor and actor agree on the fee terms, as well as other terms. However, the Fees exception does apply when fulling requests in one of the "alternative manners" I described in the Content and Manner exception. For this exception, the rule specifically defines the term *"electronic access,"* and it means 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. The excluded fees condition prohibits charging patients, their personal representatives or other individual or entity (e.g., third-party app) designated by the patient to receive his or her EHI via electronic access. An actor can charge fees to provide an individual access to his or her EHI through some other form of physical media, such as paper copies where EHI is printed out or where EHI is collated and copied to a CD or flash drive. This would not be a practice that implicates the information blocking provision, provided the fee(s) charged for that access comply with the HIPAA Privacy Rule. The rule does not limit fees and/or profits related to providing the

technology necessary for access, exchange, or use of information outside the scope of EHI. Prior to October 6, 2022, the Fees conditions in this exception apply to just the limited EHI identified by the data elements represented in the USCDI standard.

The Fees exception will typically apply to fees being charged by health IT vendors of certified health IT or HINs/HIEs to their customers in connection with providing the interoperability elements and services to enable access, exchange, and use of the customers' EHI. The other category of fees would be related to patient access to their EHI through electronic access as the term is defined under this exception, and such fees are prohibited. While most health care providers do not develop, provide and charge for interoperability elements that enable access, exchange, or use of EHI, they do have vendors charging them for these capabilities, so providers should be familiar with this exception as it provides some protections for them against excessive and unreasonable vendor (rent seeking) fees for interoperability and connectivity or for exporting their patients' EHI to move to another vendor's system.

Licensing Exception

- Addresses an actor's practices to license interoperability elements for EHI to be accessed, exchanged, or used and all the following conditions must be met by the actor:
  - Negotiating a license conditions
  - Licensing conditions
  - Additional conditions relating to the provision of interoperability elements

Actors will need to assess whether any of their existing licensing contracts or agreements contravene the information blocking provisions and specifically the Licensing exception and had to make any necessary amendments to come into compliance with the information blocking provision by April 5, 2021. If an actor does not license interoperability elements, this exception is not applicable.

There are three conditions under the Licensing Exception and an actor's practice will need to meet all the conditions to be in compliance with this exception if they license interoperability elements. The Licensing Exception would usually only apply to health IT developers of certified health IT unless other actors own and control interoperability elements related to access, exchange or use of EHI and have the ability to confer rights to the IP. These other actors may be licensees of a health IT vendor's IP related to interoperability elements and therefore should be familiar with this exception and their rights when it comes to negotiating and entering into licensing agreements for interoperability elements they need to enable access, exchange, and use of EHI.

Since the licensing exception is usually not applicable to providers and given the limited time, I will not be going into the details of the licensing exceptions conditions. I included the details for the negotiating a license and licensing conditions, and the additional conditions related to provisioning interoperability elements is provided in the Appendix.

Consumer Third-Party Applications

"Interfering with" versus *"educating"* when it comes to patients choosing a third-party application to access and receive their EHI

Practices to educate individuals would not likely interfere with the access, exchange, and use of EHI if they meet certain criteria:

- Information provided by actor must focus on any current privacy and/or security risks posed by the technology or third-party developer of the technology
- Information provided is factually accurate, unbiased, objective, and not unfair or deceptive
- Information is provided in a non-discriminatory manner

May not prevent patient from deciding to use an app despite the risks noted regarding app itself or practices of third-party developer

Discuss concern health care providers have with health IT developers that are not subject to HIPAA privacy and security rules and how providers can educate but not interfere with a patient's choice of consumer apps with which a patient decides to share his or her EHI.

ONC encourages providers to educate their patients on what to consider in choosing a consumer app when it comes to the privacy and security of their data if this is done in an unbiased, fair, objective and consistent fact-based manner. For instance, it would be ok for a provider organization or health IT vendor to ask third-party app developers about their privacy and security practices when registering their apps and then sharing that information with patients when they request or give authorization for the app to access their EHI.

Information Blocking Enforcement

- Information Blocking provision applicability date: April 5, 2021
- Cures Act authorizes HHS' Office of the Inspector General (OIG) to investigate claims of information blocking
- OIG released its proposed rule on April 24 addressing enforcement and civil monetary penalties (CMPs, up to $1M per violation) for information blocking
  - CMPs only apply to health IT developers of certified health IT and HINs/HIEs
  - OIG will refer health care providers who violate the information blocking provision to the appropriate agency to be subject to appropriate disincentives
    - HHS Secretary will address provider disincentives through future notice and comment rulemaking
- OIG has not yet released its final rule

All individuals or entities that meet the definition of actor under the information blocking provision are subject to this provision beginning April 5, 2021 and may be investigated by the HHS Office of Inspector General if they are the subject of a claim of information blocking.

Any analysis of an information blocking claim will require consideration of the individual facts and circumstances, including whether the practice or activity that interfered with access, exchange and use of EHI was required by law, whether the provider had requisite knowledge, and whether one or more exceptions apply. Failing to meet the conditions of an exception does not mean a practice is information blocking, only that it would not have guaranteed protection from penalties or disincentives and would be evaluated on case-by-case basis by the OIG for level of impact, intent, and knowledge. Health care providers found to have committed information blocking are subject to penalties; however, the penalties or disincentives for health are providers have not been addressed yet by HHS through rulemaking.

The Cure's Act authorizes the HHS Office of the Inspector General or OIG to enforce the information blocking requirements and impose civil monetary penalties or CMPs. CMPs only apply to health IT developers or certified health IT and health information networks and health information exchanges. A health care provider would be subject to CMPs if the provider met the definition of an HIN or HIE when conducting a practice that violated the information blocking provision.

OIG does not intend to investigate every information blocking complaint filed. As with other conduct they have authority to investigate, OIG has the discretion to choose which complaints to investigate. To maximize efficient use of their resources, OIG shared in their proposed rule release on April 24 that they plan to focus on selecting cases for investigation that are consistent with enforcement priorities. Based on their current expectations, they stated their enforcement priorities will include conduct that:

1) resulted in, is causing, or had the potential to cause patient harm;
2) significantly impacted a provider's ability to care for patients;
3) was of long duration;
4) caused financial loss to Federal health care programs, or other government or private entities; or
5) was performed with actual knowledge or intent.

OIG said their priorities will evolve as they gain more experience investigating information blocking.

While health care providers are not subject to information blocking CMPs, many must currently comply with separate statutes and regulations related to information blocking. Prior to the enactment of the Cures Act, Congress enacted the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), which, in part, requires a health care provider to demonstrate that it has not knowingly and willfully taken action to limit or restrict the compatibility or interoperability of Certified EHR Technology. To implement these provisions, the CMS established and codified attestation requirements to support the prevention of information blocking, which consist of three statements containing specific representations about a health care provider's implementation and use of Certified EHR technology. As part of CMS' final interoperability rule published on May 1, 2020 as well, CMS will began publicly reporting on providers and hospitals that attest negatively to the attestation requirements under the associated MACRA rules.

Once HHS completes future notice and comment rulemaking that addresses provider disincentives, the OIG will refer health care providers who violate the information blocking provision to the appropriate agency to be subject to appropriate disincentives.

Explain ONC's enforcement authority and discretion versus OIG's.
ONC has enforcement over the Health IT certification program and Conditions of Certification and Maintenance. This applies to health IT vendors with certified health IT products. They have no enforcement authority over the Information Blocking provision.

OIG will begin enforcement of information blocking and CMPs no sooner than the date actors are subject to the information blocking provisions. The applicability date for the information blocking provision was November 2, 2020 in ONC's Cures Act Final Rule and was changed to April 5, 2021 in ONC's Interim Final Rule.

Key Takeaways/ Actions

- Review relevant release of information, privacy, security, health IT policies, practices, and procedures for alignment with the requirements of the information blocking provision / exceptions
  - Ensure currency, completeness, and accuracy
- Review status of your certified health IT interoperability elements / configuration settings and adjust accordingly
- Confer with compliance officer, legal counsel, IT department, health IT vendor as appropriate to address organization-specific needs
- Establish procedures for documenting any reasons and applicable exceptions for not fulfilling or a delay in fulfilling a patient's request for EHI
- Develop internal education on any revised policies, practices, and procedures to ensure all staff are aware of changes and requirements

Educational Series Schedule

Additional Ask the Experts sessions will be scheduled based on member interest. We welcome your suggestions! HCCN@chcanys.org

Month	Topic	Webinar Date	Ask the Experts (ATE) Date(s)	
November 2021	**Cures Act Overview**	**Wed, Nov 10** Noon-1 ET	All roles **Wed, Nov 17** Noon-1 ET	
December	**OpenNotes Overview**	**Wed, Dec 1** Noon-1 ET	Providers **Wed, Dec 15** Noon-1 ET	
January 2022	**Information Blocking Exceptions**	**Wed, Jan 12** Noon-1 ET	Compliance, HIM **Tue, Jan 18** Noon-1 ET	
February	**Preparing for Cures Act Regulatory Compliance, Part 1** (organizational readiness)	**Wed, Feb 16** Noon-1 ET	Compliance, HIM, IT **Wed, Feb 23** Noon-1 ET	
March	**Preparing for Cures Act Regulatory Compliance, Part 2** (communication of records)	**Wed, Mar 16** Noon-1 ET	Providers **Wed, Mar 23** Noon-1 ET	Compliance, HIM, IT **Wed, Mar 23** 2-3 ET

Before we move to Q&A…

Contact Info

Denise Webb

- Glidepath Consulting LLC
- Email: denise@glidepathconsulting.llc
- Phone: 608-358-9115

Appendix

Preventing Harm Exception: Type of Risk Condition

Risk determined by a licensed health care professional

- Made on individualized basis in exercise of professional judgment
- Current or prior care relationship with patient

Risk arising from misidentified or mismatched, corrupt, or erroneous data

When it comes to patient safety and sharing EHI, there are two types of risk conditions. First, the risk of harm to a patient or other person determined by a licensed health care professional and second, the risk of harm to a patient or other person that arises from data that is known or reasonably suspected to be misidentified or mismatched, or corrupt due to technical failure, or erroneous for another reason.

For a risk harm determined by a licensed health care professional, this determination must be made on an individualized basis in the exercise of the provider's professional judgment and the provider must have a current or prior care relationship with the patient. Actors other than the licensed health care professional who makes the determination (HIN/HIEs or hospitals) could implement practices based on organizational policy to rely on such determination upon becoming aware of the determination and until such time they become aware the determination has been reversed or revised.

A risk of harm arising from data issues is less individualized and as a result may be identified by clinicians or other persons with relevant expertise, including but not limited to biomedical informaticists who are not licensed health care professionals. Nothing in this exception condition requires the involvement of a licensed health care professional with a care relationship to any patients whose data may be affected by practices in the design of, or decision to implement, practices an actor reasonably believes will substantially reduce a risk arising from data issues.

A provider can implement a practice that is likely to or does interfere with access. exchange, or use of EHI and qualify for the Preventing Harm exception to information blocking, if the practice is implemented to substantially reduce either a determination of risk of harm by a health care professional or a risk of harm that arises from a data issue.

Of note, the rule does not require specific or unique documentation requirements for the risk determinations by the health care professional. ONC wanted to avoid potentially duplicative or other unnecessary burdens on licensed health care professionals or other actors. Providers are already capturing documentation in the EHR or other reliable business records consistent with the HIPAA Privacy Rule and applicable state laws. ONC did suggest that information relevant to determinations would include the facts or circumstances that substantially informed each determination, and any other decision-making information the provider may otherwise have difficulty recalling or reconstructing if later asked to explain how or why they reached an individualized determination in a particular case. ONC did confirm that documenting a determination in an EHR is considered an appropriate approach to document and retain documentation on determination of risk by a licensed health care provider.

Preventing Harm Exception: Type of Harm Condition

1. Substantial harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with access, use, or exchange of a patient's EHI by his/her legal representative
    - Type of harm is substantial harm to patient or another person
    - Risk of harm is determined by a health care professional

2. Substantial harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with a patient's or his/her legal representative's access, use, or exchange of the patient's EHI that references another person
    - Type of harm is substantial harm to another person referenced in EHI other than a health care provider
    - Risk of harm is determined by a health care professional

Harm standard in this exception must be a harm that could serve as grounds for a covered entity to deny access to an individual's PHI pursuant to HIPAA.

This exception's structure essentially aligns with the harm standards in the HIPAA reviewable grounds for denial of access to PHI and addresses four types of circumstances or scenarios regarding the type of harm standard that applies. Three establish the harm standard that applies to types of circumstances specific to a patient's and his or her representative's access to the patient's EHI. The last establishes the harm standard applicable in all other types of circumstances where it is legally permissible for a requestor other than the patient or his or her personal representative to access, exchange, or use the patient's EHI.

The exception accounts for an additional risk of harm type which I already covered, that of a risk of harm that arises due to a known data issue with the EHI which can occur in electronic PHI.

Additional background detail:
Harm standards applicable to this exception align with the Privacy Rule harm standard (i) below in most circumstances and the harm standards (ii) and (iii) below in particular circumstances.

Reviewable grounds for denial (45 CFR 164.524(a)(3)). A licensed health care professional has determined in the exercise of professional judgment that:

(i) The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).
(ii) The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
(iii) The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person.
Note that a covered entity may not require an individual to provide a reason for requesting access, and the individual's rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is not a permitted reason to deny access. In addition, a covered entity may not deny access because a business associate of the covered entity, rather than the covered entity itself, maintains the PHI requested by the individual (e.g., the PHI is maintained by the covered entity's electronic health record vendor or is maintained by a records storage company offsite).

Carrying Out the Denial

If the covered entity denies access, in whole or in part, to PHI requested by the individual, the covered entity must provide a denial in writing to the individual no later than within 30 calendar days of the request (or no later than within 60 calendar days if the covered entity notified the individual of an extension). See 45 CFR 164.524(b)(2). The denial must be in plain language and describe the basis for denial; if applicable, the individual's right to have the decision reviewed and how to request such a review; and how the individual may submit a complaint to the covered entity or the HHS Office for Civil Rights. See 45 CFR 164.524(d).
If the covered entity (or one of its business associates) does not maintain the PHI requested, but knows where the information is maintained, the covered entity must inform the individual where to direct the request for access. See 45 CFR 164.524(d)(3).
The covered entity must, to the extent possible and within the above timeframes, provide the individual with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access. See 45 CFR 164.524(d)(1). Complexity in segregating the PHI does not excuse the obligation to provide access to the PHI to which the ground for denial does not apply.

Review of Denial

If the denial was based on a reviewable ground for denial and the individual requests review, the covered entity must promptly refer the request to the designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether to reaffirm or reverse the denial. The covered entity must then promptly provide written notice to the individual of the determination of the reviewing official, as well as take other action as necessary to carry out the determination. See 45 CFR 164.524(d)(4).

Preventing Harm Exception: Type of Harm Condition

3. Danger to life or physical safety harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with a patient's access, use, or exchange of his/her EHI

- Type of harm is to life or physical safety of patient or another person
- Risk of harm is either determined by a health care professional or arises from a data integrity issue

4. Danger to life or physical safety harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with a legally permissible access, use, or exchange of EHI not described in 1-3 above

- For example, access, exchange, or use of EHI by health care providers furnishing services to the patient and type of harm is to life or physical safety of patient or another person
- Risk of harm is either determined by a health care professional or arises from a data integrity issue

Privacy Sub-Exception: Pre-condition not satisfied

- To qualify for this privacy sub-exception, must meet all the following conditions:
  - Practice must be implemented in a consistent and non-discriminatory manner
  - Organizational policies and procedures or case-by-case basis
  - Precondition for access, exchange, or use of EHI relies on a consent or authorization
  - Did not improperly encourage or induce the individual to withhold consent or authorization
  - Uniform policies and procedures adopted and consistently applied to address the more restrictive preconditions when multi-state providers are subject to multiple laws with inconsistent preconditions

This sub-exception relates to federal or state law requiring a precondition be met before sharing the EHI. All conditions must be satisfied.

A provider will not be engaging in information blocking if the provider does not provide access, exchange, or use of EHI because a necessary precondition required by law is not satisfied. This sub-exception will apply to all instances where a provider's ability to provide access, exchange, or use is "controlled" by a legal obligation to satisfy a condition, or multiple conditions, prior to providing that access, exchange, or use. The nature of the preconditions the provider must satisfy will depend on the laws that regulate the provider. For example, a provider regulated by a more restrictive state law may need to satisfy more preconditions than a provider regulated by less restrictive state laws.

Providers must have written organizational policies and procedures. For any practice that doesn't conform to a provider's organization policies and procedures, the provider must document on a case-by-case basis how it reached its decision including any pre-condition criteria that were not met and why

Providers must use reasonable efforts within their control to provide the individual with a consent or authorization form when the form is required. If a provider receives a consent or authorization form that requires the provider's assistance to satisfy missing elements that are not required by law and the provider does not provide the assistance, the provider may be engaged in information blocking.

Examples that illustrate this sub-exception and would justify not providing access, exchange, or use of an individual's EHI:

Not being able to obtain consent of the individual required by certain federal and state laws for their EHI to be accessed, exchanged, or used for specific purposes, such as state laws requiring an individual's consent for uses and disclosure of EHI regarding sensitive health conditions, (i.e., HIV/AIDS, mental health, or genetic testing).
An individual's refusal to provide a HIPAA authorization required by law prior to providing access, exchange, or use of EHI.
The provider is unable to verify the identity or authority of a person requesting access to EHI and such verification is required by law before providing access, exchange, or use of EHI.
Another health care provider is requesting EHI for a quality improvement project that requires verification by the provider holding the information that the requestor has a relationship with the person whose information is being requested and the provider is unable to establish if the relationship exists.
The final rule suggests that a provider should carefully evaluate the state and federal law requirements imposed upon them and that the provider's responses are tailored to the legal precondition which protect and promote the privacy of EHI.

Privacy Sub-Exception: Health IT developer of certified health IT not covered by HIPAA

- Non-covered actors under HIPAA that are actors under the information blocking provision can avail themselves of the Privacy Exception
  - Example: a health IT developer of certified health IT offering a health IT product or service not regulated by the HIPAA Privacy Rule, such as a consumer app for diabetes control
- Practice implemented according to a process described in an organizational privacy policy and disclosed to individuals and entities before they agree to use and begin using the product or service. Privacy policy must:
  - Comply with applicable state and federal laws
  - Be tailored to specific privacy risk or interest being addressed
  - Be implemented in a consistent and non-discriminatory manner

This sub-exception relates to when a health IT developer of certified health IT is not covered by the HIPAA Privacy Rule, but their product or service is subject to the information blocking provision.

When engaging in a practice that promotes the privacy interests and interferes with access, exchange, and use of EHI, a non-covered actor must implement the practice according to a process described in its organizational privacy policies, disclose the policies to individuals and entities that use the actor's product or service before they agree to use the product or service, and the actor's privacy policies must:

(1) comply with applicable state and federal laws;
(2) be tailored to the specific privacy risk or interest being addressed; and
(3) be implemented in a consistent and non-discriminatory manner to meet this sub-exception.

Privacy Sub-Exception: Denial of individual's right of access to EHI

- Permits a covered entity or business associate to deny an individual's request for his or her EHI consistent with 45 CFR 164.524(a)(1) and (2)
- Section 164.524(a)(1) includes:
  - Psychotherapy notes and
  - Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding
- Section 164.524(a)(2) which addresses unreviewable grounds for the following denials:
  - PHI excepted from right of access in 164.524(a)(1) listed above
  - An inmate's request to obtain a copy of PHI
  - An individual's access to PHI created or obtained in course of research that includes treatment
  - An individual's access to PHI contained in records subject to the Privacy Act
  - An individual's access to PHI obtained from someone other than a health care provider under a promise of confidentiality

This sub-exception relates to when a covered entity or business associate denies an individual's request for access to his or her EHI

Complete text of 164.524(a)(2)
(i) PHI excepted from the right of access in 164.524(a)(1)
(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.
(v) An individual's access may be denied if the protected health information was

obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Privacy Sub-Exception: Respecting individual's request not to share

- Provider can elect to not provide access, exchange, and use of an individual's EHI upon an individual's request. Must meet following conditions:
  - Individual makes the request orally or in writing
    - No improper encouragement or inducement by the provider
  - Provider documents request within a reasonable time period
  - Provider may terminate individual's request for a restriction not to share the individual's EHI only if:
    - Individual requests termination in writing or agrees to termination in writing; or
    - Individual orally agrees to termination and provider documents the oral agreement; or
    - Provider informs the individual it is terminating the agreement

This sub-exception relates to not providing access, exchange, or use of EHI pursuant to an individual's request.

Bullet 1: Unless otherwise required by law, a provider can elect to not provide access, exchange, and use of an individual's EHI upon an individual's request and qualify for this sub-exception.

Note: In the case where a provider informs an individual it is terminating the agreement, the termination is not effective to the extent prohibited by law and is only applicable to EHI created or received after the provider informs individual.

The final rule does not require a specific form of documentation by the provider and indicates a note in the certified EHR or similar notation is sufficient.

Health IT Performance Exception – Conditions

Maintenance and improvement of health IT

- Implemented no longer than necessary
- Implemented in a consistent and non-discriminatory manner
- Consistent with service level agreements (SLAs) for planned or unplanned downtime or for unplanned downtime agreed to

The maintenance and improvement of health IT condition covers activities and practices a health care provider conducts to maintain, improve or upgrade the performance of the health IT infrastructure and applications under the provider's control. It also includes activities that may degrade the performance of the infrastructure or applications, but not necessarily result in an outage of services and unavailability of all EHI.

Under this condition, the following requirements must be met to qualify for the health IT performance exception.

First the outage or degradation must be for a period of time no longer than necessary to complete the maintenance or upgrades. This gives the provider or other actor under this rule flexibility for the provider to consider a variety of factors in each case and decide what would be an appropriate period of time to complete the work.

Second, outages and degradations for maintenance and improvements must be implemented in a consistent and non-discriminatory manner. For example, a health IT vendor of certified health IT that hosts an EHR for its customers, must implement outages and degradations in a consistent, non-discriminatory manner across its customers.

Finally, if the unavailability or degradation of infrastructure or applications impacting access, exchange, or use of EHI are initiated by the health IT vendor, HIE, or HIN, any planned outages must be consistent with the service level agreements between the customers of the services and the health IT vendor, HIE or HIN. For unplanned outages or degradations, these must also be consistent with the SLAs or

agreed to by the customer of the services. For example, if your health care organization uses a certified EHR hosted by the vendor, your organizations should have SLAs in place with the vendor for planned and unplanned outages. A new release to modules in your EHR would be an example of a planned upgrade done in accord with an existing SLA. Applying an emergency application patch would be an example of an unplanned outage where these are either done in accord with the SLA or by notifying and obtaining agreement from the customer of the services. For health care providers that have their own internal IT department hosting, operating and maintaining their infrastructure, network and applications, the provider organization would be expected to have downtime policies and procedures and/or service level agreements.

Health IT Performance Exception – Conditions

- Assured level of performance and actions of third-party applications
  - Implemented no longer than necessary
  - Implemented in a consistent and non-discriminatory manner
  - Consistent with service level agreements (SLAs), if applicable

The assured level of performance condition under the health IT performance exception addresses situations where a third-party application is operating or behaving in a way that does not pose a security risk but negatively impacts the performance of an actor's network, servers, or core functions of other applications. The actor can take action to shut down the application or otherwise degrade the application that is impacting the health IT performance as long as it only for the time necessary to resolve the problem with the application. The practice implemented in this scenario also must be implemented consistently and in a non-discriminatory manner. The action taken must also be consistent with any existing SLAs with the vendor of the third-party application is applicable.

Health IT Performance Exception – Conditions

- Intersection with Promoting Harm and Security exceptions
  - Must comply with conditions of these exceptions when applicable

The last condition of this exception addresses the intersection of health IT performance with the preventing harm and security exceptions. The health IT Performance exception expressly does not apply for maintenance and improvements aimed at preventing harm to a patient or other person, or to security-related practices and instead the actor's practices would need to comply with the Preventing Harm and Security exceptions, respectively. For example, if an individual or an application is making or attempting unauthorized access to systems or EHI, the actor with control of the system subject to the security risk should take prompt action to address the risk which include health IT downtime or degradation. An example of this was the Wannacry malware that hit several hospital and health system networks a few years ago.

Infeasibility Exception – Conditions

1. Uncontrollable events beyond a provider's control
   - Natural or human-made disaster
   - Public health emergency
   - Public safety incident
   - War
   - Terrorist attack
   - Civil insurrection
   - Strike or other labor unrest
   - Telecommunications or internet service interruption
   - Act of military, civil or regulatory authority

The first is uncontrollable events. These are events that are beyond a providers control and listed on this slide. If any of these events prevents a provider from providing access, exchange, or use of EHI, then that is all that is necessary to meet the infeasibility exception and no consideration of factors must be demonstrated or proven by the provider. COVID-19 and Hurricane Katrina examples.

Infeasibility Exception – Conditions

2. Segmentation
   - Patient preference
   - Required by law
   - In accordance with Preventing Harm Exception

The next condition under the infeasibility exception is segmentation. The segmentation condition would apply in cases where the provider receives a request for access, exchange, or use of EHI, and the provider is required to withhold certain EHI and the provider cannot unambiguously segment the EHI that has to be withheld from the EHI that is provided. The withholding of certain EHI could be due to a patient's preference, a law or to prevent harm in accordance with the Preventing Harm Exception.

Infeasibility Exception – Conditions

3. Request is infeasible under the circumstances
   - Requires a contemporaneous written record or other documentation of provider's consideration of specified factors
   - Must respond to the requestor within 10 business days of the receipt of request in writing with the reason(s) why
     - No specificity on level of detail

The infeasibility under the circumstances condition is helpful to providers with limited technical capability to provide access, exchange, and use of EHI in a technical manner requested or an alternative technical manner.

A provider who demonstrates prior to responding to the requestor that the request would be infeasible under the circumstances can qualify for the infeasibility exception. The rule requires the provider to do this through a written record or other documentation of its consideration of specified factors. The written record must be contemporaneous (i.e., the actor cannot use a post-hoc rationalization claiming the request was infeasible under circumstances that were not considered at the time of the request). I will cover the factors a provider must address in its determination a that a request for EHI is infeasible for the provider to fulfill on next slide. The provider/actor has 10 days from date of request to complete its written record of determination and provide the requestor a written response that the request was infeasible under the circumstances.

Infeasibility Exception – Conditions

4. Request infeasible under the circumstances (continued)
   - Factors provider must consider and address in its determination
     - Type of EHI and purposes for which it may be needed
     - Cost of complying with the request in the manner requested
     - Financial, technical, and other resources available to provider
     - Whether the provider provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship
     - Whether provider owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged
     - Why provider was unable to provide access, exchange, or use of EHI consistent with the Content and Manner exception
   - Must apply factors in a consistent and non-discriminatory manner

Cover the factors a provider must address in its determination that a request for EHI is infeasible for the provider to fulfill and how the factors must be implemented/applied in a consistent and non-discriminatory manner.

We need to remember that the information blocking provision is about whether providers are knowingly interfering with or preventing the access, exchange, and use of electronic PHI without a legitimate reason or because the law requires it. Providers still have an obligation to respond to requests for PHI in a designated record set in accordance with HIPAA for an authorized release of information or an individual's right of access and comply with their state/local laws as well, whether the PHI is electronic or not.

Fees Exception – Conditions

- Basis of fees condition – fees must be:
  - Based on objective and verifiable criteria uniformly applied for all similarly situated persons and requests
  - Reasonably related to the costs of providing the type of access, exchange, or use to or at the request of the person or entity to whom the fee is charged
  - Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied or for whom the technology is supported
  - Based on costs not otherwise recovered for same instance of service to a provider and third party

Fees an actor charges for its interoperability elements and/or services must be:
1) Based on objective and verifiable criteria uniformly applied for all similarly situated persons and requests
2) Reasonably related to the costs of providing the type of access, exchange, or use to or at the request of the person or entity to whom the fee is charged
3) Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied or for whom the technology is supported
4) Based on costs not otherwise recovered for the same instance of service to a provider and third party

Fees Exception – Conditions

- Basis of fees condition – fees may NOT be based on:
  - Whether requestor is a competitor, potential competitor, or will be using EHI in a way that facilitates competition with actor
  - Sales, profit, revenue, or other value requestor or other persons derive or may derive from access, exchange, or use of the EHI
  - Costs incurred due to a non-standard health IT design or implementation to access, exchange, or use EHI, unless requestor agreed to fees
  - Costs associated with intangible assets other than actual development or acquisition costs of such assets
  - Opportunity costs unrelated to access, exchange, or use of EHI
  - Costs leading to creation of intellectual property (IP), if actor charged a royalty for that IP in accord with Licensing Exception and royalty included development costs for IP creation

The fees an actor's charges for its interoperability elements and/or services cannot be based on:
1) Whether requestor is a competitor, potential competitor, or will be using EHI in a way that facilitates competition with actor
2) Sales, profit, revenue, or other value requestor or other persons derive or may derive from access, exchange, or use of the EHI
3) Costs incurred due to a non-standard health IT design or implementation to access, exchange, or use EHI, unless requestor agreed to fees
4) Costs associated with intangible assets other than actual development or acquisition costs of such assets
5) Opportunity costs unrelated to access, exchange, or use of EHI
6) Costs leading to creation of intellectual property (IP), if actor charged a royalty for that IP in accord with Licensing Exception and royalty included development costs for IP creation

Fees Exception – Conditions

- Excluded fees condition – this condition prohibits:
  - Fees prohibited by HIPAA under a patient's right to PHI
  - Fees based in any part on the electronic access of an individual's EHI by the individual, personal representative, or another person or entity (e.g., third-party consumer-facing app) designated [authorized] by the individual.
  - Fees to perform an export of EHI via health IT certified to the EHI export criteria for purposes of switching health IT products or to provide patients their EHI
  - Fees to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired

The following fees are prohibited under the excluded fees condition:
1) Fees prohibited by HIPAA under a patient's right to PHI
2) Fees based in any part on the electronic access of an individual's EHI by the individual, personal representative, or another person or entity (e.g., third-party consumer-facing app) designated [authorized] by the individual

Remember that electronic access under this exception means 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, assuming the actor can provide the EHI in this manner. If an individual requests her EHI in another form and format or manner other than electronic access as defined here, then any fees charged must not be fees prohibited by HIPAA under a patient's right of access to his or her PHI. For example, a patient could request her EHI be emailed via secure email and if the covered entity has the technical capability to readily producible the EHI in the format requested and to email securely, the covered entity should do so and is permitted to charge a cost-based fee that complies with HIPAA

3) Fees to perform an export of EHI via health IT certified to the EHI export criteria for purposes of switching health IT products or to provide patients their EHI
4) Fees to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired

Example that would not meet the conditions of this exception: a health care

provider that charges individuals a fee in order that the individuals be given access to their EHI via the health care provider's patient portal or another mode of web-based delivery, would not be able to benefit from this exception. Similarly, where an individual authorizes a consumer-facing app to retrieve EHI on the individual's behalf, it would be impermissible for an actor to charge the app or its developer a fee to access or use APIs that enable access to the individual's EHI.

Licensing Exception – Conditions

- Negotiating a license conditions
  - Must begin negotiations within 10 days of receipt of request
  - Must complete license negotiations in good faith, subject to licensing conditions, within 30 days of receipt of request
  - Documentation on negotiation not required but highly suggested

When responding to a request for a license to interoperability elements needed to enable access, exchange, or use of EHI, the actor must begin licensing negotiations within 10 days of receipt of request and make a good faith effort to complete negotiations in accord with the licensing conditions within 30 days of receipt of the request. If negotiations fail, having some documentation will be helpful in case of an information blocking claim and investigation but is not required in the rule.

Note that for an actor to consider licensing its interoperability elements, the requestor would need to have a legitimate claim to the underlying, existing EHI for which the interoperability element would be necessary for access, exchange, or use and is seeking to interoperate with the actor or the actor's customers. So, there must be a nexus between requestor's need to license an interoperability element and existing EHI on one or more patients. If not, the actor does not need to consider licensing the interoperability element requested in accordance with the Licensing Exception. There must be actual EHI at stake for the actor to need to seek coverage under this exception.

Licensing Exception – Conditions

- Licensing conditions
  - Scope of rights
  - Reasonable royalty
    - May not charge a royalty for IP that led to creation of the IP if the actor recovered any development costs pursuant to the Fees Exception
  - Non-discriminatory terms
    - Price and non-price, including royalty terms
    - Based on objective and verifiable criteria and applied uniformly for all similarly situated classes of persons and requests
    - Must not be based on whether requestor is a competitor or potential competitor, or will be using EHI obtained via the interoperability elements in a way that facilitates competition
    - Must not based on revenue or other value requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements

Scope of rights: license must provide all rights necessary to: (1) enable the access, exchange, or use of EHI; and (2) achieve the intended access, exchange, or use of EHI via the interoperability element

Reasonable royalty: If an actor charges a royalty for the use of interoperability elements, the royalty base and rate must be reasonable. The reasonableness of any royalties would be based solely on the basis of the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information. In evaluating the actor's assertions and evidence that the royalty was reasonable, the ONC and OIG may consider several factors that are listed in the final rule and are covered in the information blocking provision cheat sheet summary posted on the CHIME policy web page. Note that fees for creating the IP cannot be recovered both under the Fees exception and then again under the royalty fees under the Licensing exception.

Non-discriminatory terms: The terms on which an actor licenses and otherwise provides interoperability elements must be non-discriminatory. This requirement would apply to both price and non-price terms, and thus would apply to the royalty terms as well as other types of terms that may be included in licensing agreements or other agreements related to the provision or use of interoperability elements. Terms must be based on objective and verifiable criteria and be applied uniformly for all similarly situated classes of persons and requests. An actor cannot choose to

license an interoperability element to one requestor and then refuse to or impose different licensing terms to license the same interoperability element to a second similarly situated requestor.

The terms must not be based on whether the requestor is a competitor or potential competitor or will be using EHI obtained via the interoperability elements in a way that facilitates competition with the actor. Nor can the terms be based on revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements.

Licensing Exception – Conditions

- Licensing conditions (continued)
  - Collateral terms – the actor must NOT require the licensee or its agents or contractors to do or agree to do any of the following:
    - Not compete with or deal exclusively with actor in any product, service, or market
    - Obtain additional licenses, products, or services not related to or can be unbundled from the requested interoperability elements
    - License, grant, assign, or transfer the licensee's own IP to the actor
    - Pay a fee of any kind unless the fee meets requirements of royalty condition or satisfies the requirements in the Fees Exception

Collateral terms – the actor must NOT require the licensee or its agents or contractors to do or agree to do any of the following:
1) Not compete with or deal exclusively with actor in any product, service, or market
2) Obtain additional licenses, products, or services not related to or can be unbundled from the requested interoperability elements
3) License, grant, assign, or transfer the licensee's own IP to the actor
4) Pay a fee of any kind unless the fee meets requirements of royalty condition or satisfies the requirements in the Fees Exception

Licensing Exception – Conditions

- Licensing conditions (continued)
  - Non-disclosure agreements (NDA)
    - May require a licensee to agree to a confidentiality or non-disclosure agreement to protect its trade secrets, provided it s no broader than necessary to prevent the unauthorized disclosure of its trade secrets
    - Agreement must identify the specific information it claims as trade secrets and information must meet definition of a trade secret under applicable law

The actor licensing its intellectual property may require the licensee to execute a confidentiality agreement or NDA, but the rule does not require it. If the actor requires an NDA to protect its trade secrets from unauthorized disclosure, then the agreement must be no broader than necessary and must identify the specific information it claims are trade secrets, and the information must meet the definition of a trade secret under applicable law.

Licensing Exception – Conditions

- Additional conditions relating to the provision of interoperability elements The actor cannot:
  - Engage in a practice that has purpose or effect of impeding the efficient use of the interoperability elements to access, exchange, or use EHI for any permissible purpose
  - Impede the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand
  - Degrade the performance or interoperability of a licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability

Information Block Glossary of Terms

- **Information Blocking**
  - If conducted by a health provider, a practice likely to interfere with access, exchange or use of electronic health information (EHI) when the provider knows that such practice is unreasonable and is likely to interfere with access, exchange or use of EHI
- **Actors**
  - Individuals and entities covered by the information blocking provision, i.e., health care providers, health IT developers of certified health IT, health information networks, and health information exchanges
- **Consumer Third-Party Application**
  - Applications developed by third parties authorized and used by patients to access, exchange and use their electronic health information
- **Certified Health IT**
  - A health IT product that meets the certification requirements under the ONC Health IT Certification Program. Requirements for certification are established by standards, implementation specifications and certification criteria adopted by the Secretary at the Department of Health and Human Services (HHS)

Information Block Glossary of Terms

- **Vendor**
  - An external entity that delivers goods and services to the healthcare organization and to patients on behalf of the healthcare organization
- **Health IT developer of certified health IT**
  - An individual or entity that develops or offers health information technology and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health IT (one or more) certified under the ONC Health IT Certification Program
- **Health Information Network (HIN)/ Health Information Exchange (HIE)**
  - Individual or entity that determines, controls, or has discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology for access, exchange, or use of EHI: (1) Among more than two unaffiliated individuals or entities (other than individual or entity to which this definition might apply) that are enabled to exchange with each other; and (2) Is for a treatment, payment, or health care operations (TPO) purpose regardless of whether individuals or entities are subject to 45 CFR 160 and 164.

Information Block Glossary of Terms

- **Designated Record Set**
  - The set of information that a patient is required to have access to, such as medical and billing records, case management and health plan enrollment. Includes records that are used "to make decisions about individuals" also are included; this definition is not fully defined by the ONC but is addressed in an ONC FAQ
- **Electronic Health Information (EHI)**
  - The electronic protected health information (ePHI) in a designated record set (as defined in the Health Insurance Portability and Accountability Act (HIPAA) regulations) regardless of whether the records are used or maintained by or for a covered entity
- **Interoperability**
  - Health information technology that (a) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; (b) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and (c) does not constitute information blocking

Information Block Glossary of Terms

- **United States Core Data for Interoperability (USCDI)**
  - A standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.(see Content and Manner slide for full list of data elements)
- **Electronic Access**
  - An internet-based method that makes EHI available at the time the electronic health information is requested and where no manual effort is required to fulfill the request