The 21st Century Cures Act and Information Blocking Webinar

January 21, 2021
Introductions

David Ginsberg  
Co-founder and President of PrivaPlan  
Cybersecurity Lead Consultant for BlueNovo

Han Ashley  
Associate at PrivaPlan & BlueNovo

Fernan Caparas  
Chief Technology Officer of BlueNovo

Huzefa Dossaji  
Telemedicine & BD Lead of BlueNovo
Overview-21 Century CURES

The rule is designed to give patients and their healthcare providers secure access to health information. It also aims to increase innovation and competition by fostering an ecosystem of new applications to provide patients with more choices in their healthcare.

- It calls on the healthcare industry to adopt standardized application programming interfaces (APIs), which will help allow individuals to securely and easily access structured electronic health information using smartphone applications.

- The rule includes a provision requiring that patients can electronically access all of their electronic health information (EHI), structured and/or unstructured, at no cost.

- Finally, to further support access and exchange of EHI, the rule implements the information blocking provisions of the Cures Act. The rule outlines eight exceptions to the definition of information blocking.
Overview-21 Century CURES

“We explained in the Proposed Rule that 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 (84 FR 7508).”
“We have finalized the definition of “access” as “the ability or means necessary to make EHI available for exchange, use, or both” (§ 171.102). This final definition improves on the proposed definition (see 84 FR 7601) in a couple of ways. First, it makes clear that “access” is the ability or means necessary to make EHI available not only for “use,” but also for “exchange” or both (the proposed definition only included “for use”). This modification will provide clarity because, as we noted in the Proposed Rule, these terms are interrelated and EHI cannot be exchanged or used if it is inaccessible. Second, to be responsive to comments and in order to promote additional clarity in the definition, we have removed “including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained” from the definition. This language was exemplary and resulted in some confusion among stakeholders. Last, we clarify that the definition of “access” is not limited to direct interfaces, which we believe is evident by the final definition.”
“We have finalized the definition of “exchange” as “the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks.” As with the finalized “access” definition, we have maintained the general scope of the proposed definition while modifying the definition for clarity. First, we removed “securely and efficiently” as proposed descriptors of the way that EHI is to be transmitted under the definition. While we continue to advocate for and promote secure and efficient exchange, we do not think this descriptive language is necessary within the definition of “exchange” because “exchange” for the purposes of the information blocking provision can occur regardless of whether the transaction is “secure” or “efficient.” Our intent with this definition was never to exclude unsecure or “inefficient” exchanges from the definition or enforcement of the information blocking provision because the exchange of EHI was not secure or “inefficient,” so we have removed this extraneous language. We also refer stakeholders to the information blocking exceptions included in this final rule that discuss how EHI may be transmitted and the importance of security as it relates to the access, exchange, and use of EHI.

Second, we have removed the provision at the end of the proposed definition, that in order for “exchange” to occur, it must be “in a manner that allows the information to be accessed and used.” This language was potentially confusing because the manner of transmittal is not a necessary component of the “exchange” definition. If EHI is exchanged but is done so in a way that does not permit the use of the EHI, then that practice may implicate the information blocking provision because the “use” of the EHI is being prevented. Further, to be responsive to comments, we emphasize that “transmitted” within the definition is not limited to a one-way transmission, but instead is inclusive of all forms of transmission such as bi-directional and network-based transmission. We note this as a point of clarification, as it was always our intent that “transmission” would be interpreted this way.”
KEY PRINCIPLES-USE

“We have finalized “use” to mean “the ability for EHI, once accessed or exchanged, to be understood and acted upon.” Put another way, “use” is an individual or entity’s ability to do something with the EHI once it has been accessed or exchanged.

• IT to access relevant EHI; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose
INFORMATION BLOCKING

(a) Information blocking means a practice that—
(1) Except as required by law or covered by an exception, is likely to interfere with access, exchange, or use
• of electronic health information; and
• (2) If conducted by a health information technology developer, health information network or health information exchange, such developer, network or exchange knows, or should know, that such practice is likely to interfere with, access, exchange, or use of EHI; or
• (3) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.

• (b) Until 24 months after the publication date of the final rule, EHI for purposes of paragraph (a) of this section is limited to the EHI identified by the data elements represented in the USCDI standard adopted in § 170.213.
WHAT MAKES AN ACTOR AN INFORMATION BLOCKER?

Elements of information blocking

• Actor regulated by the information blocking provision
• Involves electronic health information (EHI)
• Practice is likely to interfere with, access, exchange, or use of EHI
• Requisite knowledge by the actor
• Not required by law
• Not covered by an exception
WHO IS AN ‘ACTOR’?

• Healthcare Providers

• Health IT Developers of Certified Health IT

• Health Information Networks/Health Information Exchanges
  • *Is a health center controlled network a health information network?* A PCA?
  • *Is an EPIC or Cerner Community model a HIN?*
“Electronic Health Information”

The final rule:

- Focused the scope of EHI to mean electronic protected health information (ePHI) to the extent that the ePHI is included in a designated record set as these terms are defined for HIPAA.

- This is applicable whether the actor is a covered entity or not.
Designated Record Sets—the forgotten HIPAA Privacy Rule requirement:

“A group of records maintained by or for a covered entity that is:

• (i) The medical records and billing records about individuals maintained by or for a covered health care provider;

• (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

• (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

• (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.”
INFORMATION SUBJECT TO THIS RULE

• Designated Record Sets form the basis of data that is accessible to a patient or subject individual under the HIPAA Privacy Rule and now under Information Blocking

• The Designated Record Set can include ePHI and non “e” PHI

• Importance of defining the Designated Record Set and documenting this---
INFORMATION SUBJECT TO THIS RULE

The rule also incorporates the US Core Data for Interoperability and HL7 FHIR as data and transmission standards for exchange of data between actors and-

Further promotes the use of Application Program Interfaces for a user-friendly approach to data sharing
The USCDI

United States Core Data for Interoperability

Version 1 (July 2020 Errata)
The USCDI is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.

- A USCDI “Data Class” is an aggregation of various Data Elements by a common theme or use case.
- A USCDI “Data Element” is the most granular level at which a piece of data is represented in the USCDI for exchange.
# USCDI v1 SUMMARY OF DATA CLASSES AND DATA ELEMENTS

<table>
<thead>
<tr>
<th><strong>Allergies and Intolerances</strong></th>
<th><strong>Immunizations</strong></th>
<th><strong>Problems</strong></th>
<th><strong>Vital Signs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Substance (Medication)</td>
<td>Immunizations</td>
<td>Problems</td>
<td>Diastolic Blood Pressure</td>
</tr>
<tr>
<td>Substance (Drug Class)</td>
<td></td>
<td></td>
<td>Systolic Blood Pressure</td>
</tr>
<tr>
<td>Reaction</td>
<td></td>
<td></td>
<td>Body Height</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Body Weight</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Heart Rate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Respiratory Rate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Body Temperature</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pulse Oximetry</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Inhaled Oxygen Concentration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BMI Percentile (2 - 20 years)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Weight-for-length Percentile (Birth - 36 Months)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Head Occipital-frontal lobe circumference</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Percentile (Birth - 36 Months)</td>
</tr>
<tr>
<td><strong>Assessment and Plan of Treatment</strong></td>
<td><strong>Laboratory</strong></td>
<td><strong>Procedures</strong></td>
<td></td>
</tr>
<tr>
<td>Assessment and Plan of treatment</td>
<td>Tests</td>
<td>Procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Values/Results</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Care Team Members</strong></td>
<td><strong>Medications</strong></td>
<td><strong>Provenance</strong></td>
<td></td>
</tr>
<tr>
<td>Care Team Members</td>
<td>Medications</td>
<td>Author Time Stamp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Author Organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Clinical Notes</strong></td>
<td><strong>Patient Demographics</strong></td>
<td><strong>Smoking Status</strong></td>
<td></td>
</tr>
<tr>
<td>Consultation Note</td>
<td>First Name</td>
<td>Smoking Status</td>
<td></td>
</tr>
<tr>
<td>Discharge Summary Note</td>
<td>Last Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>History &amp; Physical</td>
<td>Previous Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Imaging Narrative</td>
<td>Middle Name (including middle initial)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laboratory Report Narrative</td>
<td>Suffix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pathology Report Narrative</td>
<td>Birth Sex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure Note</td>
<td>Date of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Progress Note</td>
<td>Race</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethnicity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preferred Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Current Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Previous Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Number Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td><strong>Unique Device Identifier(s) for a Patient’s Implantable Device(s)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Goals</td>
<td>Unique Device Identifier(s) for a Patient’s Implantable Device(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Health Concerns</strong></td>
<td><strong>Provenance</strong></td>
<td><strong>Unique Device Identifier(s) for a Patient’s Implantable Device(s)</strong></td>
<td></td>
</tr>
<tr>
<td>Health Concerns</td>
<td>Author Time Stamp</td>
<td>Unique Device Identifier(s) for a Patient’s Implantable Device(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Author Organization</td>
<td>Unique Device Identifier(s) for a Patient’s Implantable Device(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to protect an individual’s privacy, provided certain conditions are met.

Objective of the Exception:

- This exception recognizes that if an actor is permitted to provide access, exchange, or use of EHI under a privacy law, then the actor should provide that access, exchange, or use. However, an actor should not be required

- to use or disclose EHI in a way that is prohibited under state or federal privacy laws.

Key Conditions of the Exception

- To satisfy this exception, an actor’s privacy-protective practice must meet at least one of the four sub-exceptions:

  - Precondition not satisfied: If an actor is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing access, exchange, or use of EHI, the actor may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied under certain circumstances.

  - Health IT developer of certified health IT not covered by HIPAA: If an actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, the actor may choose to interfere with the access, exchange, or use of EHI for a privacy-protective purpose if certain conditions are met.

  - Denial of an individual’s request for their EHI consistent with 45 CFR 164.524(a) (1) and (2): An actor that is a covered entity or business associate may deny an individual’s request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) of the HIPAA Privacy Rule.

  - Respecting an individual’s request not to share information: An actor may choose not to provide access, exchange, or use of an individual’s EHI if doing so fulfills the wishes of the individual, provided certain conditions are met.
“Denial of an individual’s request for their EHI consistent with 45 CFR 164.524(a) (1) and (2): An actor that is a covered entity or business associate may deny an individual’s request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) of the HIPAA Privacy Rule.”

164.524 incorporates numerous exclusions to release of PHI including psychotherapy notes, criminal or civil proceedings, and:

“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.”

And preventing harm . . .
EXCEPTIONS TO INFORMATION BLOCKING-HARM THRESHOLD

An actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm will not be considered information blocking when:

(a) **Reasonable belief.** The actor engaging in the practice must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person that

- would otherwise arise from the access, exchange, or use of electronic health information affected by the practice. For purposes of this section, “patient” means a natural person who is the subject of the electronic health information affected by the practice.

- (b) **Practice breadth.** The practice must be no broader than necessary to substantially reduce the risk of harm that the practice is implemented to reduce.

(c) **Type of risk.** The risk of harm must:

- (1) Be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose electronic health information is affected by the determination; or

- (2) Arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

(d) **Type of harm.** The type of harm must be one that could serve as grounds for a covered entity (as defined in § 160.103 of this title) to deny access (as the term “access” is used in part 164 of this title) to an individual’s protected health information under:

- (1) Section 164.524(a)(3)(iii) of this title where the practice is likely to, or in fact does, interfere with access, exchange, or use (as these terms are defined in § 171.102) of the patient’s electronic health information by their legal representative (including but not limited to personal representatives recognized pursuant to 45 CFR 164.502) and the practice is implemented pursuant to an individualized determination of risk of harm consistent with paragraph (c)(1) of this section;
EXCEPTIONS TO INFORMATION BLOCKING-HARM THRESHOLD

An actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm will not be considered information blocking when:

Patient right to request review of individualized determination of risk of harm. Where the risk of harm is consistent with paragraph (c)(1) of this section, the actor must implement the practice in a manner consistent with any rights the individual patient whose electronic health information is affected may have under § 164.524(a)(4) of this title, or any Federal, State, or tribal law, to have the determination reviewed and potentially reversed.

- Practice implemented based on an organizational policy or a determination specific to the facts and circumstances. The practice must be consistent with an organizational policy that meets paragraph (f)(1) of this section or, in the absence of an organizational policy applicable to the practice or its use

- in particular circumstances, the practice must be based on a determination that meets paragraph (f)(2) of this section.

- (1) An organizational policy must:
  - (i) Be in writing;
  - (ii) Be based on relevant clinical, technical, and other appropriate expertise;
  - (iii) Be implemented in a consistent and non-discriminatory manner; and
  - (iv) Conform each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use.
EXCEPTIONS TO INFORMATION BLOCKING-HARM THRESHOLD

An actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm will not be considered information blocking when:

• A determination must:

• (i) Be based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use; and

• (ii) Be based on expertise relevant to implementing the practice consistent with the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use in particular circumstances.
EXCEPTIONS TO INFORMATION BLOCKING-HARM THRESHOLD

Do you currently follow and maintain procedures related to the Privacy Harm language? Many organizations fail to do so!!

Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

• (i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or (iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
On December 10, 2020 a new NPRM was released that if adopted could change the definition of professional judgement . . .
It will not be information blocking for an actor to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.

Objective of the Exception:

• This exception is intended to cover all legitimate security practices by actors, but does not prescribe a maximum level of security or dictate a one-size-fits-all approach.

Key Conditions of the Exception

• The practice must be:
  • Directly related to safeguarding the confidentiality, integrity, and availability of EHI;
  • Tailored to specific security risks; and

• Implemented in a consistent and non-discriminatory manner.

• The practice must either implement a qualifying organizational security policy or implement a qualifying security determination.
EXCEPTIONS TO INFORMATION BLOCKING-INFEASIBILITY

It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met.

Objective of the Exception:

• This exception recognizes that legitimate practical challenges may limit an actor’s ability to comply with requests for access, exchange, or use of EHI. An actor may not have—and may be unable to obtain—the requisite technological capabilities, legal rights, or other means necessary to enable access, exchange, or use.
EXCEPTIONS TO INFORMATION BLOCKING-HEALTH IT PERFORMANCE

Health IT Performance Exception - Key Conditions of the Exception

• The practice must meet one of the following conditions:

• Uncontrollable events: The actor cannot fulfill the request for access, exchange, or use of electronic health information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.

• Segmentation: The actor cannot fulfill the request for access, exchange, or use of EHI because the actor cannot unambiguously segment the requested EHI.

• Infeasibility under the circumstances: The actor demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances.

• The actor must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.
EXCEPTIONS TO INFORMATION BLOCKING

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

- 171.301 Content and manner exception—when will an actor’s practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information not be considered information blocking?

- 171.302 Fees exception—when will an actor’s practice of charging fees for accessing, exchanging, or using electronic health information not be considered information blocking?

- 171.303 Licensing exception—when will an actor’s practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?
EXCEPTIONS TO INFORMATION BLOCKING-CONTENT AND MANNER

An actor’s practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information will not be considered information blocking when the practice meets all of the following conditions.

• (a) Content condition—electronic health information. An actor must respond to a request to access, exchange, or use electronic health information with—
  • (1) USCDI. For up to May 2, 2022, at a minimum, the electronic health information identified by the data elements represented in the USCDI standard adopted in § 170.213.
  • (2) All electronic health information. On and after May 2, 2022, electronic health information as defined in § 171.102.

Manner condition—(1) Manner requested. (i) An actor must fulfill a request described in paragraph (a) of this section in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

• (ii) If an actor fulfills a request described in paragraph (a) of this section in any manner requested:
  • (A) Any fees charged by the actor in relation to fulfilling the response are not required to satisfy the exception in § 171.302; and
  • (B) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303.
2) *Alternative manner.* If an actor does not fulfill a request described in paragraph (a) of this section in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner, as follows:

- (i) The actor must fulfill the request without unnecessary delay in the following order of priority, starting with paragraph (b)(2)(i)(A) of this section and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in a paragraph.

- (A) Using technology certified to standard(s) adopted in part 170 that is specified by the requestor.

- (B) Using content and transport standards specified by the requestor and published by:

  - (1) The Federal Government; or

  - (2) A standards developing organization accredited by the American National Standards Institute.

- (C) Using an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor.

- (ii) Any fees charged by the actor in relation to fulfilling the request are required to satisfy the exception in §171.302.

- (iii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is required to satisfy the exception in §171.303.
EXCEPTIONS TO INFORMATION BLOCKING-FEES

An actor’s practice of charging fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using electronic health information will not be considered information blocking when the practice meets the conditions in paragraph (a) of this section, does not include any of the excluded fees in paragraph (b) of this section, and, as applicable, meets the condition in paragraph (c) of this section.

• Basis for fees condition. (1) The fees an actor charges must be—

• (i) Based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;

• (ii) Reasonably related to the actor’s costs of providing the type of access, exchange, or use of electronic health information to, or at the request of, the person or entity to whom the fee is charged;

• (iii) Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported; and

• (iv) Based on costs not otherwise recovered for the same instance of service to a provider and third party.

• (2) The fees an actor charges must not be based on—

• (i) Whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor;

• (ii) Sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, or use of the electronic health information;
EXCEPTIONS TO INFORMATION BLOCKING-FEES

• iii) Costs the actor incurred due to the health IT being designed or implemented in a non-standard way, unless the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use the electronic health information;

• (iv) Costs associated with intangible assets other than the actual development or acquisition costs of such assets;

• (v) Opportunity costs unrelated to the access, exchange, or use of electronic health information; or

• (vi) Any costs that led to the creation of intellectual property, if the actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.

• (b) Excluded fees condition. This exception does not apply to—

• (1) A fee prohibited by 45 CFR 164.524(c)(4);

• (2) A fee based in any part on the electronic access of an individual’s EHI by the individual, their personal representative, or another person or entity designated by the individual;

• (3) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; and

• (4) A fee to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired.

• (c) Compliance with the Conditions of Certification condition. Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4), § 170.404, or both of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

• (d) Definition of Electronic access. The following definition applies to this section:

Electronic access means an internet-based method that makes electronic health information available at the time the electronic health information is requested and where no manual effort is required to fulfill the request.
EXCEPTIONS TO INFORMATION BLOCKING-LICENSING

An actor’s practice to license interoperability elements for electronic health information to be accessed, exchanged, or used will not be considered information blocking when the practice meets all of the following conditions.

• (a) *Negotiating a license conditions.* Upon receiving a request to license an interoperability element for the access, exchange, or use of electronic health information, the actor must—

• (1) Begin license negotiations with the requestor within 10 business days from receipt of the request; and

• (2) Negotiate a license with the requestor, subject to the licensing conditions in paragraph (b) of this section, within 30 business days from receipt of the request.

• (b) *Licensing conditions.* The license provided for the interoperability element(s) needed to access, exchange, or use electronic health information must meet the following conditions:

• (1) *Scope of rights.* The license must provide all rights necessary to:

• (i) Enable the access, exchange, or use of electronic health information; and

• (ii) Achieve the intended access, exchange, or use of electronic health information via the interoperability element(s).

... Etc.
COMPLIANCE AND ENFORCEMENT

Actors that are subject to the information blocking regulations may be investigated by the HHS Office of Inspector General if they are the subject of a claim of information blocking. Further, actors found to have committed information blocking are subject to penalties:

- Health IT developers of certified health IT, health information networks, and health information exchanges → Civil monetary penalties (CMPs) up to $1 million per violation
- Health care providers → Appropriate disincentives to be established by the Secretary
What will the organizational and administrative requirements be?

How does the 21st Century Cures Act tie with HIPAA?
What will the organizational and administrative requirements be?

1. Which workflows need review and modification
2. Which policies and procedures need to be updated
What are the EHR and IT systems requirements?

Does your organization know what the Vendor requirements are?
What should I expect from our EHR vendor?

- Do you have visibility?
- Is this process streamlined?
QUESTIONS?

Contact Huzefa Telehealth & BD Lead at BlueNovo
Huzefa.Dossaji@bluenovo.com
Phone: (504) 400-7473

or visit our website at www.bluenovo.com
WHY BLUENOVO?

Proven TCO & ROI - Market leader in cost and value. Focus on process and technologies that improve revenue, provider productivity & reduce costs.

Strategic & Operational Orientation - Keen understanding of FQHC strategic needs and provision of best in-class service.

Experienced Teams - Right-fit BlueNovo support teams with deep FQHC experience, assigned and dedicated to supporting your staff.

Technology in FQHCs - In-depth technical knowledge suited to supporting community-based healthcare organizations.

Security Focused – Comprehensive leading edge security offerings to protect valuable data assets.

Future Focused - Deployment of scalable & reliable technological solutions to day-to-day health center challenges.

Clinical Best Practices - Bringing lessons learned and best practice experience to the toughest IT & Health IT challenges.

Proactive Monitoring & Maintenance – Ongoing monitoring to eliminate downtime and business impact.

BlueNovo Client Family - Be connected to our network of highly satisfied network of community-based healthcare organizations to collaborate on similar challenges and share best practices.

www.bluenovo.com

Proprietary & Confidential