Information Blocking Requirements Under the 21st Century Cures Act

By: William P. Hassett, Esq.

The Department of Health and Human Services Office of the National Coordinator of Health Information Technology's (ONC) Final Rule on electronic health record interoperability and electronic health information blocking provisions contained in the 21st Century Cures Act is set to take effect on **April 5, 2021**.[1] With 95 percent of hospitals and over 85 percent of office base practices using electronic health records, the information blocking provisions of the Cures Act will have a direct impact on nearly all healthcare providers. This article will provide an overview of the information blocking provisions of the Cures Act, how it applies to healthcare providers and considerations for compliance with the Cures Act's complex regulatory requirements.

The 21st Century Cures Act

The 21st Century Cures Act was passed by Congress in December of 2016. The robust legislation encompasses many aspects of healthcare including the allocation of funds for the development of treatments and medications, combating the opioid crisis and the restructuring the Food and Drug Administration to expediate approval of new drugs and devices.

A smaller yet equally important component of the Cures Act seeks to improve interoperability between electronic health records (EHR) and to promote access, exchange and use of electronic health information (EHI) among patients, providers, payers and technology developers. The new requirements in the ONC Final Rule will take effect April 5, 2021 and apply to "Actors" defined in the Cures Act as healthcare providers, health IT developers, health information networks (HIN) and health information exchanges (HIE).[2]

The Access, Exchange and Use of Electronic Health Information

Passed by Congress over 20 years ago, the Health Insurance Portability and Accountability Act (HIPAA) federally mandated that an individual had the right to request and receive protected health information (PHI) from healthcare providers. This right was reenforced by the Health Information Technology for Economic and Clinical Health Act (HITECH) which stated that an individual now had the right to obtain a copy of PHI in electronic format (ePHI) from a healthcare provider that utilized EHR. Under HITECH, an individual could also direct a healthcare provider to transmit the record to a designated third person and limited fees imposed for the transmission/duplication to labor costs (not copying costs).[3]

[1] https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification
[2] 45 CFR §171.102
[3] 42 USCA §17935 (e)

The Cures Act builds upon HIPAA and HITECH by supporting a patient's ability to request secure access, exchange and use ePHI via smartphone applications or computer software.[4] The ONC Final Rule sets forth guidance and requirements for healthcare providers, health IT developers, HIEs and HINs to develop and implement technology and protocols to facilitate this goal. This includes the elimination of conduct that constitutes information blocking.

Information Blocking

The Cures Act broadly defines "information blocking" as "a practice that - except as required by law or covered by an exception . . . is likely to interfere with access, exchange or use of electronic health information."[5] With respect to patients, an example of information blocking could be placing restrictions on when EHI may be accessed or limitations on the scope of EHI that is patient accessible. Information blocking could also occur when a patient becomes "locked in" to using a particular technology or healthcare network because their EHI is not portable.

Information blocking is not just limited to patient requests for access to EHI, it also occurs when a healthcare provider is unable to access a patient record from another provider or encounters restrictions on accessing health information exchanges via their office EHR. Information blocking can also occur when a provider looks to switch EHR platforms and encounters contractual limitations from the prior vendor on the use and exchange of medical information.

Notably, the Cures Act definition of information blocking makes an important distinction between health care providers and IT developers, HINs or HIEs.[6] A healthcare provider can only engage in information blocking <u>where he or she knows that the practice is unreasonable or is likely to interfere</u> with the access, exchange or use of EHI. In contrast, information blocking conducted by health IT developers, HINs and HIEs are practices that these actors know or <u>should know is likely to interfere</u> with the access, exchange or use of EHI. The distinction is subtle but significant as it requires a healthcare provider to have a conscious state of mind that their conduct is unreasonable or likely to interfere with access to EHI whereas for health IT developers, HINs and HIEs it is assumed that they should know the conduct engaged in likely constituted information blocking. A requirement that a healthcare provider *had knowledge* that a practice was unreasonable is a very difficult element to establish should there be an investigation of an information blocking complaint.

Electronic Health Information

The definitions of EHI in the Cures Act regulations is synonymous with the definition for electronic protected health information in a designated record set as defined in the Health Insurance Portability and Accountability Act (HIPAA). For a healthcare provider, this constitutes a patient's medical record including but not limited to demographics, progress notes, laboratory results, diagnostic tests as well as billing information. Like HIPAA regulations, psychotherapy notes are excluded from disclosure as EHI under the Cures Act.

---

[4] See, 45 CFR §171.102 *Access* – means the ability or means necessary to make EHI available for exchange or use; *Exchange* – means the ability for EHI to be transmitted between and among different technologies, systems, platforms or networks; *Use* – means the ability for EHI, once accessed or exchanged to be understood and acted upon.

[5] 45 CFR § 171.103(a)(1)

[6] 45 CFR §171.103(a)(2)(3)

Notably, between the dates of April 5, 2021 and October 6, 2022, an actor under the Cures Act must respond to a request to access, exchange or use EHI with, *at a minimum*, all requested EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI).[7] This interim policy on the definition of EHI was put in place as EHR vendors are presently updating their products to support the access, exchange, and use of all data elements in the USCDI and this will be a time-consuming process. After October 6, 2022, an actor (healthcare provider, health IT developer, HIN and HIE) must respond to request for EHI pursuant to the electronic protected health information definition contained in HIPAA that was adopted by the Cures Act.

Exceptions Where Information Blocking is Permitted

By its definition, information blocking does not include instances where EHI access is restricted due to compliance with state and federal laws. A healthcare provider's continued compliance with laws that place restriction on the release of health information will not be considered information blocking under the Cures Act. An example of where a restriction of access would not constitute information blocking are areas of special confidentiality that require a specific patient consent before release such as mental health, drug/alcohol treatment and/or HIV treatment.

In addition to compliance with laws, the ONC Final Rule defined eight exceptions that will not be considered information blocking so long as all accompanying conditions are satisfied.[8] The ONC stressed however that when an actor does not meet all the conditions of an exception, it will not automatically constitute information blocking. Such instances of partial compliance will be considered on a case-by-case basis to determine whether information blocking has occurred.

The eight exceptions identified by the ONC were divided into two categories: exceptions that involve failures in responses to requests for access, exchange or use of EHI and exceptions that involve procedures for fulfilling requests to access, exchange or use EHI.

Exceptions that involve failures in response to requests for access:

1. *Preventing Harm* – it will not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or other person. The practitioner's satisfaction of this exception includes a reasonable belief that blocking the information will substantially reduce the risk of harm. The EHI that is withheld must also be no broader than necessary.
2. *Privacy* – information blocking will not occur if an actor does not fulfill a request for access, exchange or use of EHI to protect an individual's privacy so long as conditions are met. For example, pursuant to HIPAA regulations and New York State laws a patient may be required to provide an authorization before EHI is released to a third party.
3. *Security* – It will not be information blocking for an actor to interfere with the access, exchange or use of EHI to protect the security of EHI. To qualify under this exception, the information blocking must be directly related to safeguarding the confidentiality, integrity and availability of EHI. The restrictions must

[7] 45 CFR §171.103(b) the USCDI defines standardized data elements that must be documented in an EHR whereas the HIPAA definition describes what information is accessible. With respect to the contents of a patient medical record the definitions are typically synonymous. *See also*, United States Core Data for Interoperability Version 1 https://www.healthit.gov/isa/sites/isa/files/2020-10/USCDI-Version-1-July-2020-Errata-Final_0.pdf

[8] 45 CFR §171.200

also be tailored to meet specific security risks and implemented in a consistent and non-discriminatory manner.

4. *Infeasibility*- if the actor does not have the technological capabilities or legal rights to respond to a request for access, exchange or use of EHI it will not be considered information blocking. To invoke this exception, the practitioner must meet one of the following conditions: uncontrollable events (disaster, public emergency), segmentation (cannot segment the requested EHI), or infeasibility under the circumstances (a practitioner must demonstrate through a written record the factors that led to infeasibility).
5. *Health IT Performance* – it will not be information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health ITs performance for the benefit of the overall performance of the health IT. Again, ONC provided conditions that must be met to satisfy this exception including that the IT measures must be implemented for a time no longer than necessary and must be implemented in a consistent and non-discriminatory manner.

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

6. *Content and Manner* – It will not be information blocking for an actor to limit the content of its response to a request to access, exchange or use EHI or the manner in which it fulfills a request to access, exchange or use EHI, provided certain conditions are met.
7. *Fees* – Actors may charge fees, including fees that result in a reasonable profit margin for accessing, exchanging and using EHI so long as prescribed conditions are met. ONC stressed however that this exception to information blocking was intended to promote and enhance technologies for interoperability while not protecting rent seeking, opportunistic fees and exclusionary practices.
8. *Licensing* – This exception is most likely applicable to vendors. It will not be information blocking for an actor to license interoperability elements for EHI to be accessed, exchanged or used. This exception allows actors to protect the value of their innovations and charge reasonable royalties. Again, conditions must be met such as the negotiation of licensing conditions that include scope of rights, reasonable royalties and non-discriminatory terms.

Enforcement and Penalties

Enforcement of the Cures Act will be handled by the Department of Health and Human Services Office of the Inspector General (OIG).[9] Notably, the Cures Act mandates that health IT developers, HINs HIEs will be subject to civil monetary penalties of up to $1 million per violation of information blocking.[10] In contrast, healthcare providers will be subject to "appropriate disincentives" that were not defined in the Cures Act or Final Rule and have yet to be determined by the OIG.[11]

Enforcement of civil monetary penalties will not begin until they are established by the rule making of OIG which to date has not been released. As a result, actors will not be subject to penalties until a civil monetary penalty

[9] 42 USCA §300jj-52(b)(1)

[10] 42 USCA § 300jj-52 (b)(2)(A) In its determination of a penalty the OIG shall take into account factors such as the nature and extent of the information blocking and harm that resulted including the number of patients affected, number of providers affected, and the number of days information blocking persisted.

[11] 42 USCA §300jj-52 (b)(2)(B)

rule is final. In the interim, OIG will exercise discretion relative to the enforcement of information blocking incidents that may occur.

Considerations for Compliance with the Cures Act Information Blocking Provision

Although the information blocking requirements become effective on April 5, 2021, the regulations and the ONC Final Rule are very complex and will take a significant amount of time to be fully implemented. That said, healthcare practitioners should be proactive in their approach to compliance which will be multiple factorial and require input from medical, legal and information technology staff or consultants. A good starting point for any evaluation would be a careful review of existing policies and procedures concerning the release of EHI. Here are some considerations:

- Conduct a review of HIPAA privacy and security policies and focus on whether there are any impediments to requests for access, exchange or use of EHI that would constitute information blocking. Based on the ONC final rule, when a patient makes a request for access, a healthcare provider will need to allow access office notes, laboratory or diagnostic reports as soon as they are electronically available to the practice. Therefore, policies requiring that a healthcare provider must review laboratory or diagnostic test results before they are made available may need to be reconsidered. Similarly, a practitioner should guard against prematurely releasing EHI that is incomplete. Office notes should not be made subject to request for access until they are signed by the practitioner to ensure completeness and accuracy.
- Consult with Information Technology staff or consultants to the determine the capabilities of existing platforms to allow the access, exchange or use of EHI without creating the opportunity for a security breach.
- Consult with EHR vendors to confirm that appropriate action is being taken to ensure compliance with the information blocking rules. Discussions should include the ability of the EHR to support data segmentation per a patient request or regulation (e.g., limitations on HIV or mental health records) and distinguishing between parts of the health record that are subject to the Cures Act EHR definition and those that are not such as personal notes and observations.
- Review existing contracts or business associate agreements with vendors to determine if they implicate the information blocking regulations.
- Educate staff regarding information and requests for access, exchange or use of EHI. In most instances, these individuals will be the first to receive such requests or complaints about limitations to access, exchange or use. Staff must be made aware of the information blocking requirements and how to proceed when presented with a request pertaining to EHI.

Conclusion

The interoperability and information blocking provisions of the Cures Act will provide unprecedented access, exchange and usage of EHI to patients and all healthcare actors alike. However, this expansion is accompanied by complex regulatory requirements that will impact nearly all healthcare providers. Restrictions on conduct that could constitute information blocking will require a multifaceted review of existing policies and procedures to ensure compliance.