Information Blocking: A Practical Perspective

FEDERAL RULES PROHIBIT PROVIDERS AND VENDORS FROM INTERFERING WITH ACCESS TO OR SHARING OF ELECTRONIC HEALTH INFORMATION

By Erica Ash, JD; Wakaba Tessier, JD; and Kelsey Toledo, JD

On May 1, 2020, the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC) released its final rule on **information blocking** as part of the 21st Century Cures Act. The Final Rule applies to health care providers, health information technology developers (subject to ONC's Health IT Certification Program), health information networks and health information exchanges. It prohibits these entities from unreasonably interfering with the access, exchange or use of electronic health information (EHI). HHS extended the original compliance date, which was November 2, 2020, to April 5, 2021.

WHAT IS INFORMATION BLOCKING?

Information blocking is generally 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. The entity has actual knowledge—or in the case of health IT developers, health information networks or health information exchanges, should know—that the practice is unreasonable and is likely to interfere with, prevent or materially discourage access, exchange or use of EHI. Until October 6, 2022, electronic health information is limited to the subset of EHI represented by the data elements identified by the U.S. Core Data for Interoperability (USCDI) standard.[1] On and after October 6, 2022, the information blocking regulation in 45 CFR part 171 will pertain to all EHI (as defined in 45 CFR 171.102).

> The entity has actual knowledge—that the practice is unreasonable and is likely to interfere with, prevent or materially discourage access, exchange or use of EHI.

Some examples of information blocking include:

- Hospital policies or procedures that require personnel to obtain an individual's written consent before sharing the individual's electronic health information with unaffiliated providers for treatment purposes even if obtaining such consent is not required by state or federal law.
- Contractual arrangements that prevent sharing or limit how EHI is shared with patients, their health care providers or other third parties.
- Patients or health care providers become "locked in" to a particular technology or health care network because their electronic health information is not portable.
- Charging an individual, their personal representative or another person or entity designated by the individual for electronic access to the individual's EHI.
- A health care provider has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient's health care provider but takes several days to respond.

ARE THERE ANY EXCEPTIONS TO THE INFORMATION BLOCKING RULE?

Yes. There are eight exceptions to the information blocking rule. The exceptions generally fall into two categories: 1) exceptions that involve not fulfilling requests to access, exchange or use of EHI; or 2) exceptions that involve procedures for fulfilling requests to access, exchange or use of EHI. To meet any exception under the information blocking rule, the provider or IT resource must meet all applicable requirements and conditions of the exception at all relevant times.

Here are the exceptions that involve *not fulfilling requests* to access, exchange or use of EHI:

1. Preventing harm exception.[2] It will not be information blocking for a provider or IT resource to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. This exception aligns with existing HIPAA regulations.[3]

2. Privacy exception.[4] It will not be information blocking if an entity does not fulfill a request to access, exchange or use EHI in order to protect an individual's privacy, provided certain conditions are met.

You should review existing policies and procedures relating to the use and disclosure of EHI to determine whether revisions should be made in light of the information blocking rule.

3. Security exception.[5] It would not be information blocking for an entity to interfere with the access, exchange or use of EHI in order to safeguard the confidentiality, integrity and availability of EHI, provided certain exceptions are met.

4. Infeasibility exception.[6] It will not be information blocking if an entity does not fulfill a request to access, exchange or use EHI due to the infeasibility of the request, provided certain conditions are met.

5. Health IT performance exception.[7] It will not be information blocking for an entity to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.

Here are the exceptions that involve *fulfilling requests* to access, exchange or use of EHI:

1. Content and manner exception.[8] It will not be information blocking for a provider or IT resource to limit the content of its response to requests 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.

2. The fees exception.[9] It will not be information blocking for an entity to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging or using EHI, provided certain conditions are met.

3. Licensing exception.[10] It will not be information blocking for an entity to license interoperability elements for EHI to be accessed, exchanged or used, provided that certain conditions are met.

PRACTICAL CONSIDERATIONS

Determine whether the information blocking rule applies. The definition of health care provider, health information exchange and health information network are all broad so that even if you do not think the rule applies to you, think again and make sure that that is indeed the case.[11] If the information blocking rule does in fact apply, there are steps you should be taking now to comply. Depending on whether you are a provider or an IT resource, the compliance steps you need to take will vary.

Assess risks of non-compliance. Because penalties will vary on based on what type of entity is involved and to what extent the action was information blocking, it is important to understand which role a person or organization holds under the Final Rule. For providers, ONC did not establish a mechanism for information blocking disincentives; however, providers must agree to "prevention of information blocking" in order to meet CMS' promoting interoperability (PI) reporting requirements. Furthermore, a provider may be acting in more than one role (e.g., as an IT developer, health information exchange or health information network) for the purposes of information blocking. In such cases, a violation of the information blocking rules could subject the entity to civil monetary penalties. Thus, it is important to understand how the organization or provider is functioning in order to determine possible risks of noncompliance.

Policies. As a preliminary matter, if you are a health care provider, you should review existing policies and procedures relating to the use and disclosure of EHI to determine whether revisions should be made in light of the information blocking rule. Moreover, organizations should review existing contract templates, such as business associate agreements, to access whether revisions are needed. In addition to reviewing existing policies, organizations should consider implementing policies specifically relating to information blocking. In particular, policies may focus on what the exceptions are, and who within an organization will be responsible for assessing whether and documenting when an exception to information blocking may be used.

Another important policy that every organization should implement is a policy regarding how it will enforce the information blocking prohibitions and ensure staff compliance. In part, this requires organization to address how they will identify information blocking. For example, one practice to help ensure compliance would be to audit staff who use exceptions frequently to withhold information. By conducting regular audits, the organization can show that it is diligently trying to prevent information blocking. Further, organizations should also have policies describing the sanctions and possible supplementary training for instances where providers are information blocking.

In addition, the policies should also answer the following questions:

- Who is in charge of auditing records?
- How will complaints by patients be investigated?
- Will there be a dedicated email address for inquiries?
- Who approves the use of an exception? Is it a committee or the individual?
- How will staff be informed regarding what information is being automatically sent to patients?
- How are minors' records handled? May their parents automatically have access to all their records?
- What disciplinary actions are appropriate for providers who are consistently information blocking when an exception does not apply?

Training and staff communication. As is necessary for most compliance efforts, training and staff communication on information blocking are essential. As such, organizations should implement training programs that ensure staff get the information they need on an ongoing basis, to comply with the rules and the organization's policies relating to information blocking. Training may focus on how to determine when a practice is information blocking, when an exception applies and the conditions of applicable exceptions, what will be provided to patients and other authorized requestors from the medical record that was not previously provided, and what steps to take if a staff member suspects information blocking is occurring.

CONCLUSION

New legal requirements like this information blocking rule can easily cause concerns and compliance challenges. While each organization will have differing needs, a structure for implantation and well-developed compliance plan will allow organizations to be well-prepared to prevent information blocking.

__Wakaba Tessier__ is a partner in the Kansas City office of Husch Blackwell LLP; __Erica Ash__ and __Kelsey Toledo__ are associates with the firm, all working with a variety of health care clients.

Wakaba regularly counsels clients on sensitive and highly regulated issues including health information confidentiality, mental health records, multistate recordkeeping and data transfer, and big data strategies for the creation and implementation of data warehouses. She can be reached at wakaba.tessier@huschblackwell.com.

REFERENCES

1. 45 C.F.R. § 171.103

2. 45 C.F.R. § 171.201.

3. See 45 CFR § 164.512(j).

4. 45 C.F.R. § 171.202.

5. 45 C.F.R. § 171.203.

6. 45 C.F.R. § 171.204.

7. 45 C.F.R. § 171.205.

8. 45 C.F.R. § 171.301.

9. 45 C.F.R. § 171.302.

10. 45 C.F.R. § 171.303.

11. 45 CFR 171.102 assigns the same meaning as "health care provider" at 42 U.S.C. 300jj. This "includes hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, Federally qualified health center, group practice, pharmacist, pharmacy, laboratory, physician, practitioner, provider operated by, or under contract with, the IHS or by an Indian tribe, tribal organization, or urban Indian organization, rural health clinic, a covered entity ambulatory surgical center, therapist and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary."

WALKING PROGRAM

(continued from page 16)

with PAD can include pain, fatigue and discomfort in the legs. However, other pathologies can mimic claudication," Dr. Wagner explained. "The vascular surgeon can differentiate these vascular issues. We have a variety of testing available in our offices."

SET is an effective first-line option for patients. "Not all patients need procedures or interventions. We want to give patients the choice to manage their symptoms through exercise," Dr. Wagner concluded.

For more information on Midwest Aortic & Vascular Institute, visit **www.mavi.life.**

REFERENCES

1. Society for Vascular Surgery. Peripheral Artery Disease. https://vascular.org/patient-resources/vascular-conditions/peripheral-arterial-disease

2. Collins TC, Peterson NJ, Suarez-Almazor M, Ashton CM. The Prevalence of Peripheral Arterial Disease in a Racially Diverse Population. *Arch Intern Med.* 2003;163(12):1469-1474. doi:10.1001/archinte.163.12.1469

3. Treat-Jacobson D, McDermott MM, Beckman JA. Implementation of Supervised Exercise Therapy for Patients With Symptomatic Peripheral Artery Disease *Circulation.* 2019;140:e700–e710. DOI: 10.1161/CIR.0000000000000727