Compliance Today - September 2022
The risk is coming from inside the house: Information blocking and non-EHR data

By Jennifer Vessels, JD, CHC, CHPC

- linkedin.com/in/jennifer-vessels-jd-chc-chpc-1a310176/

In the classic 1979 horror film *When a Stranger Calls*, a babysitter phones the police to report a series of increasingly threatening and frightening prank calls. The police manage to trace the calls (via the wonders of 1970s technology), resulting in the chilling and memorable line: "The calls are coming from inside the house!" While deranged callers are probably not at the top of most compliance professionals' lists of concerns, internal sources of data and, more importantly, a lack of clarity about the risks posed by that data are frightening enough to keep one up at night. In preparation for the next phase of implementation of the Information Blocking Rule, it will be critical for organizations to have a clear view of the data lurking outside of electronic health record (EHR) systems.

Background

In 2016, passage of the 21st Century Cures Act put the healthcare industry on notice of a coming sea change in how electronic health information (EHI) is to be used and shared, with the end goal of full interoperability, "allow[ing] for complete access, exchange, and use of all electronically accessible health information for authorized use."[1] To this end, the final rule, published in May 2020,[2] prohibits engaging in "information blocking," or any practices likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

April 2021 ushered in the first phase of requirements related to information blocking, focusing on 52 data elements within 16 data classes specified in the United States Core Data for Interoperability version 1.[3] A survey of 4,000 clinical, technical, and administrative stakeholders across the industry found a large percentage were unprepared for the new requirements.[4] While 70% of the respondents indicated they were aware of the rules going into effect, nearly half reported either making no changes in anticipation of the requirements or being unaware of how to ensure compliance for their facilities. Given this, it was perhaps unsurprising that the same number were unfamiliar with the term "information blocking" and/or were unaware of any practices or policies that might constitute it.

While enforcement penalties against providers have yet to be announced in the first year of implementation, the Office of the National Coordinator for Health Information Technology (ONC) received 364 claims of possible information blocking via its Report Information Blocking Portal. Over 225 of these were submitted by patients, and more than 300 were against providers.[5] This would indicate that patient claims against providers are likely to far outstrip those against health IT developers, information networks, or information exchanges. This should be a wake-up call to any organization that has not yet taken concrete steps to address the information blocking requirements.

Barring further extensions by ONC, the next phase of the requirements will go into effect October 6, 2022, and will expand the subject data to include all EHI within the designated record set, which for providers would include all medical and billing records about individuals or any other record maintained by a provider and used to make decisions about the individual. Many organizations worked hard to expand availability, use, and exchange of the data within the EHR in anticipation of the first phase of the information blocking requirements, and the October 2022 deadline may require an even deeper dive.

Do you know where your data lives?

The vast majority of patient data lies within the EHR, and facilitating easy access, use, or exchange of the information within it will go a long way to meeting obligations under the Information Blocking Rule. That said, small details and forgotten data often cause the biggest problems. In working toward full compliance with the rules, it is important to consider carefully any non-EHR data sources. A few examples:

- **Radiology information systems**: Do they integrate with the EHR? If not, can images be requested from an outside study that providers could rely on in treating patients?
- **Records from outside providers**: Is there an ability to permit access, use, or exchange of external records used by providers in diagnosis or treatment of patients? While these might not be considered part of the organization's legal medical record, they would be part of a designated record set and therefore are subject to the Information Blocking Rule.
- **Cancer or tumor registry information**: Can the organization respond to a request for copies of data it has submitted to state cancer registries?
- **Pharmacy information systems:** Is any patient-specific information stored in the pharmacy system? Is it fully integrated with the EHR? If not, how can the organization respond to a request for information located within it?
- **Case management databases:** Does the case management team document in an electronic format anywhere other than the EHR? If so, is that information easily producible in response to a request?
- **Patient billing systems**: Is the patient accounting and billing system integrated with the EHR? If not, can the organization respond to a request for detailed billing, payment, and/or claims records? These records would also be part of the designated record set and are clearly included within the information blocking regulations.
- **Legacy EHR systems**: Is there any information within a legacy EHR system that has not been integrated into the current EHR? If the data cannot be easily retrieved from such systems, has an assessment been performed regarding which exception to the Information Blocking Rule might apply?
- **Legacy billing systems**: Has patient-specific information been integrated into the current patient billing system? If not, an assessment similar to that discussed above should be performed regarding possible exceptions to the Information Blocking Rule.

Figuring out what you don't know

An organization cannot mitigate risks it doesn't know about, and its first step should be identifying and locating potential sources of EHI. Consult the organization's designated record set policy as a starting point and then develop a plan for how to proceed. Many organizations have a legal medical record policy but not a designated record set policy, and an awareness of the differences between the two will likely save organizations regulatory headaches when enforcement begins in earnest. An important caveat to the road map outlined here: This information is focused on responding to patient requests for access, use, and exchange of EHI, but that should not be the end of the analysis for any organization. Third-party requests, while likely to comprise a smaller percentage of requests, must also be accommodated under the Information Blocking Rule, and each organization should develop a process for considering and responding to them.

While the size and nature of the organization will determine the scope of any effort to identify non-EHR data, the health information management department is a good first stop, as they are likely already aware of many of the potential sources within the organization.

The next step should be a survey of the rest of the organization's departments and lines of business, along with any acquired physician practices, nonphysician patient service providers, business associates, and vendors that collect and/or maintain EHI. The survey can be as simple as a basic spreadsheet listing the responsible department, the data source, a description of the data within, and a determination as to whether it constitutes EHI.

Now that you know, what do you do with it?

Once potential sources of EHI are identified, leverage other available resources in the organization to help assess the status of current compliance and readiness to comply with the information blocking requirements effective October 6. If resources are available to assemble a task force or committee to conduct the assessment, it should include representatives from health information management and IT, of course, along with the EHR technical team, clinical representatives, legal counsel, the compliance team, financial services, and subject matter experts who can speak to the individual data sources discovered.

If a large-scale effort is not a realistic option for the organization, build on the information compiled in the spreadsheet identifying potential sources of data, adding columns for the questions below. At a minimum, these questions should be answered for each potential source:

1. Does the data constitute EHI within the definition of the Information Blocking Rule? That is, "EHI means electronic protected health information as defined in 45 C.F.R. 160.103 to the extent it would be included in a designated record set as defined in 45 C.F.R. § 164.501, regardless of whether the group of records are used or maintained by or for a covered entity," excluding psychotherapy notes and information compiled in anticipation of legal or administrative proceedings.[6] (Note: If the answer to this is "no," further assessment is not needed.)

2. Is it or can it be integrated with the EHR?

3. Is the data readily available for access if requested?

4. Is the data readily available for use if requested?

5. Is the data readily available for exchange if requested?

6. If the answer to any of questions 3–5 above is "no," does it fall under one of the eight exceptions to the information blocking requirements: preventing harm, privacy, security, infeasibility, health IT performance, content and manner, fees, and licensing?

Bear in mind there will likely be different answers for different data depending on the nature of the request, and a solid understanding of the eight exceptions will be crucial to this part of the assessment. If the organization does not have the technical feasibility to facilitate the transfer of data from a legacy EHR to a patient's requested app, perhaps the data is producible in a different electronic format. While awaiting further guidance from ONC on the specifics of the exceptions, work with stakeholders in the organization to come up with a working definition of each based on the information available and use that definition for the assessment.

Answering these questions for each of the potential sources of EHI identified within the organization will provide a solid framework to assess current compliance and readiness for the October 6 deadline and a clear indication of the highest areas of risk.

Small and solo providers, take heed

Since 2019, the Office for Civil Rights has announced nearly 30 settlements or enforcement actions under its Right of Access Initiative. Of these, half have been against small or solo practices. Given this, it seems reasonable to expect the government will not hesitate in enforcing the Information Blocking Rule against small entities, as well. Any small providers that struggled to comply with the first phase of regulations in 2021 would be well-advised to take the necessary steps to comply before the October 2022 deadline, and certainly before enforcement penalties are announced.

Conclusion

Time is running out to identify non-EHR sources of EHI before the next phase of information blocking regulations goes into effect. Identifying internal sources of EHI will help your organization *get out of the house,* assess and mitigate the risks posed, and better prepare for the October 2022 changes.

Takeaways

- The next phase of information blocking regulations goes into effect in October 2022.
- The new regulations will expand the amount and types of data required to be available for access, use, or exchange.
- Non-EHR sources of data may pose significant risk, and organizations should take steps to identify and assess potential data sources.
- Identifying data sources, while daunting at first, can be broken down into manageable steps tailored to the organization's size and resources.
- Small and solo providers should be especially diligent, given the government's recent enforcement priorities.

[1] 42 U.S.C. § 300jj(9).
[2] 45 C.F.R. § 171.
[3] "United States Core Data for Interoperability," HealthIT.gov, accessed July 1, 2022, https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.
[4] "Healthcare Organizations Unready for ONC Cures Act Final Rule," LifeImage, April 6, 2021, https://www.lifeimage.com/news/new-healthcare-industry-survey-reveals-majority-of-healthcare-organizations-unprepared-for-onc-cures-act-final-rule.
[5] "Information Blocking Claims: By the Numbers," HealthIT.gov, accessed July 1, 2022, https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers.
[6] 45 C.F.R. § 171.102.