BLOG POST / PRIVACY & SECURITY LAW BLOG

Technology + Privacy & Security

Top HHS "Information Blocking" Regulatory Compliance Challenges

By Adam H. Greene, Michaela Bantilan Andrawis, and Lyra Correa

10.05.20

As the November 2 compliance date quickly approaches, healthcare providers are finding that tackling the new "information blocking" regulations from the U.S. Department of Health and Human Services requires substantial operational and cultural changes. Davis Wright Tremaine has created an Information Blocking Toolkit to help identify and analyze potential information blocking practices that impermissibly restrict access, exchange, and use of electronic health information (EHI).

Changing the culture, however, may prove to be the more difficult endeavor. Here are five of the top information blocking challenges we are seeing, along with tips for addressing them.

1. Access to Minors' Records

During the ages in which minors can consent to certain healthcare services (such as reproductive health services), parents have a right to access some of a child's medical information but generally not that for which the child consents on his or her own. Providing just the right amount of access—no more and no less—has long proven difficult.

Providers often address this by entirely excluding medical records of such minors from patient portals. However, to knowingly interfere with a parent's access to EHI of a minor (other than the few services to which the minor may consent) may constitute information blocking.

Overly broad policies blocking access likely will not comply. If a provider cannot segment out the confidential information, then the provider may need to rely on the infeasibility exception—which requires a response in 10 days explaining why it is infeasible to segment out the data. If explaining the basis of infeasibility would expose that the minor sought confidential services, then an individualized determination to withhold information to prevent harm to the minor may be an alternative.

2. Delaying Test Results

It is common for providers to delay the release of certain test results in order to provide an opportunity to meet with the patient first. Clinicians often view this as essential to care—fearing that patients will not understand the results or will become unnecessarily distressed without understanding the appropriate context.

Providers, however, no longer will be able to have policies of knowingly delaying disclosure of lab results for certain categories of tests unless the practice is required by law. Instead, a provider must release confirmed lab results once they become available unless the patient's clinician makes an individualized determination that delaying the results will prevent harm—specifically, an endangerment to the life or physical safety of an individual. This determination likely would only apply in a small minority of cases.

3. Revisiting Confidentiality Restrictions

The Privacy Rule provides healthcare providers significant discretion in using or disclosing EHI, such as for public health or research purposes. But healthcare providers that disclose health information to third parties rarely share such latitude.

Rather, through a data use agreement, business associate agreement, or standard confidentiality restriction, providers generally seek to limit a third party's use and disclosure of EHI to only the narrow purposes of the contract or underlying services. Contractual restrictions can constitute information blocking, however.

Commentary to the regulation states that "some restrictions, while not required by law, may be reasonable and necessary for the privacy and security of individuals' EHI." But the regulation and commentary do not make clear where the line is drawn. If a healthcare provider is sharing EHI (e.g., a designated record set) with a third party and restricts the third party's uses and disclosures that are otherwise permissible under

HIPAA and state privacy law, it is not clear whether such restrictions could qualify as information blocking.

Providers likely do not need to overhaul their business associate agreements to allow the business associate to make every use or disclosure that the provider can make. But the information blocking regulations may significantly impact negotiations in years to come, as business associates may seek more latitude. Denying such requests could fall into a gray area with respect to information blocking.

4. Scanned Records of Other Providers

It is common for healthcare providers to receive copies of another provider's medical records for a patient and to scan them into their electronic medical record system as a media file for the patient. This can create numerous information blocking challenges.

First, healthcare providers may incorrectly believe that they don't have to provide access to information that was generated by another facility. There is often a belief that because they cannot vouch for the quality of the information, they should not have to provide it. But because the information has been added to their electronic medical record system and is maintained in the patient's medical record, it qualifies as EHI (subject to the temporary limitation to information that falls within the U.S. Core Data for Interoperability (USCDI) data set). Accordingly, any interference with access, exchange, or use of this data implicates information blocking.

Second, because the data is scanned rather than structured data, it may be difficult to identify to what extent it falls within the USCDI (which is the only EHI that is subject to the information blocking regulations until May 2, 2022). There is a good chance, though, that the unstructured data includes fields that fall within the USCDI. Unless the scanned data also includes information that legally cannot be provided and it is infeasible to separate the two, then interfering with access to the scanned medical records may be information blocking.

5. The Struggle to Identify All Potential Information Blocking Practices

Finally, what may be the biggest struggle is identifying all of the information blocking practices internally within an organization. A provider may have dozens of systems—both software systems and administrative systems—that are involved in the access, exchange, or use of EHI with others. For each system, there could be dozens of practices that potentially qualify as information blocking.

For electronic medical records, do clinicians have unfettered authority to mark information as confidential and interfere with the disclosure of their clinical notes? Is the availability of certain categories of test results intentionally delayed when such

delay is not required by law? Do health plans request access to patients' EHI for their own payment and healthcare operations? Do researchers request access to EHI for activities preparatory to research?

Each practice in response to such requests may implicate information blocking issues and require analysis. Our Toolkit assists with identifying and analyzing these practices—but it's still going to involve some significant sleuthing and a whole lot of time and effort. It may be best to view information blocking compliance as a continuing journey rather than a destination.

Conclusion

The above are just a small sample of the issues we are seeing arise from the information blocking regulations. The new rules also require a shift in culture. It has been over 17 years since patients gained the right to access their protected health information under the HIPAA Privacy Rule. Yet we are still seeing what I call the "A Few Good Men syndrome": clinicians seeking to withhold access because they believe patients "can't handle the truth."

Now we have regulations that essentially provide that patients' information held by providers belongs to the world, to the extent legally permitted. The compliance challenges are only beginning, and it will be a long time before everyone accepts this change in culture.

Related Posts

10.05.20
BLOG POST
Privacy Oracle

The Privacy Oracle: October 2020

10.05.20
BLOG POST
Biometrics

Facebook BIPA Settlement Moving Forward

10.05.20

BLOG POST

Data Protection

National Consumer Privacy Law Round-Up: Data Privacy and Security Are Back in Focus