COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 29, Number 39. November 02, 2020
Information-Blocking Rule Is Delayed Until April; It's a 'Pretty Huge Cultural Change'

By Nina Youngstrom

A hospital employee laughs at an email from a competitor asking for patient information for a quality assessment study. The email has a list of admissions, including patient names, dates of birth and discharge dates, and the employee is asked to match them to the hospital's patient list and the patients of unaffiliated community providers that share the hospital's electronic health records (EHRs), and then send over discharge summary notes and consultation notes for every encounter within 90 days of discharge. "There's no way I'm going to hand over so much sensitive patient information to a competitor," the employee thinks. He hits the delete button on the competitor's request.

That probably won't fly when HHS's information-blocking regulation,[1] which interprets a provision from the 21st Century Cures Act, takes effect April 5. The compliance deadline was Nov. 2, but HHS announced a delay on Oct. 29. The competing hospital in this scenario may file an information-blocking complaint with HHS. "Pressing delete on requests for patient health information could be information blocking in the years to come," said attorney Adam Greene, with Davis Wright Tremaine in Washington, D.C. The hospital could be fined $1 million in relation to denying the request for access to patient information of the unaffiliated health care providers that the hospital hosts on its EHR system. "As of [April 5], you should not be engaging in any practices that are information blocking," Greene said Oct. 15 at a webinar sponsored by the Health Care Compliance Association.[2] The enforcement regulations are not in effect yet, however, so it's unclear when penalties will be assessed.

According to the final regulation, which was published in the *Federal Register* May 1 by the HHS Office of the National Coordinator for Health Information Technology (ONC), any action or inaction that knowingly interferes with the access, exchange or use of electronic health information (EHI) may lead to "disincentives" or penalties. Information blocking won't be tolerated unless a practice is required by law or falls into one of eight exceptions. The rules apply to three types of "actors": health care providers (e.g., hospitals and physicians), health information networks/health information exchanges, and developers of certified health information technology.

'EHI Is Not Really Yours'

"This is a pretty monumental change. I don't think there's anything analogous to this anywhere," Greene said. "Culturally, this rule is essentially stating your EHI is not really yours. It's more of a public good. You can't interfere with it flowing freely to anyone who wants it unless an exception applies. That's a pretty huge cultural change from the way people currently look at their patients' health information." He said the information-blocking rules also "interfere culturally" with the way clinicians think about their patient relationships. There's a longstanding belief that patients shouldn't have their medical information until physicians talk to them about it. "The information-blocking rule prohibits a provider from delaying requested test results in order to first talk to the patient, with limited exceptions, such as a belief that physical harm will result," Greene said. "That's not going to go down well with a lot of clinicians and will be a challenge for each organization."

It may be hard to reconcile the information-blocking rule with HIPAA, with its emphasis on safeguarding protected health information (PHI). "I sometimes call this the anti-privacy law," Greene said. But there's a way through the paradox, Greene said. Privacy laws fall in one of three buckets. One is "thou shalt not disclose PHI without authorization" unless it's for treatment, payment, operations or certain other permissible purposes; the second bucket is for required disclosures (e.g., to law enforcement when treating gunshot wounds); and the third is discretionary. "In the space that's discretionary, there are a lot of disclosures that can be, but don't have to be, made," Greene said. "That's where information blocking comes in." Unless one of the eight exceptions apply, providers lose discretion and must share EHI.

How the Industry Got Here

With the information blocking compliance date coming soon, Greene encouraged providers to set compliance in motion.[3]

Greene explained how the industry got to information-blocking rules. Once upon a time, there were silos of paper records, so the federal government spent billions of dollars to move to electronic health records in the Health Information Technology for Economic and Clinical Health Act. "They didn't expect all electronic information would then be trapped in electronic silos," he said. "Congress underestimated market forces." In response, Congress addressed information blocking in the Medicare Access and CHIP Reauthorization Act (MACRA) in 2015. MACRA added three attestations to the Medicare EHR incentive payment program. Providers have to attest they're not blocking information to be eligible for payments under meaningful use (now known as promoting interoperability). Noncompliance can decrease their reimbursement, and CMS has announced it will soon post attestations on its website.

When Congress passed the 21st Century Cures Act in December 2016, it again took on information blocking. The regulation applies to EHI, which is the same as electronic PHI under HIPAA to the extent it would be included in a designated record set, Greene said. The designated record set includes medical records, billing and other records used to make decisions about people. EHI doesn't include psychotherapy notes (e.g., notes from counseling sessions that therapists take for their own reference) and information compiled in anticipation of criminal, civil or administrative actions.

Rule Has Eight Exceptions

Although the prohibition on information is sweeping, there are eight exceptions in the ONC regulation, said attorney Lyra Correa, with Davis Wright Tremaine, at the webinar. They make room for information blocking under certain circumstances. Some involve practices where actors would not fulfill requests for access, exchange or use of EHI, and the rest address procedures for fulfilling the requests.

Each exception has a set of conditions that must be fully satisfied. If providers find that a practice doesn't meet all the conditions of an exception, "the good news is it won't automatically be considered information blocking," Correa said. "But what it does mean is there is no guaranteed protection from penalties."

The exceptions are:

1. **Preventing harm**: Providers and other actors can justify practices that interfere with the access, exchange or use of EHI if they're protecting patients and other persons against unreasonable risks of harm. "The harm standard is very specific and generally" refers to the life or physical safety of an individual, Correa said.
2. **Privacy**: Information may be blocked because of a privacy requirement, such as HIPAA or state medical

privacy law. For example, a hospital may not have patient authorization to release information to an attorney, she said. "This also covers other situations involving privacy requirements, including when individuals say 'I don't want you to disclose my information.'"

3. **Security**: This covers practices implemented to safeguard the confidentiality of EHI, such as safeguards to verify patient identity. "The security exception must be implemented in a consistent and nondiscriminatory manner," Correa noted.

4. **Health information technology performance**: "This is generally for situations where you have an upgrade to or conduct maintenance on HIT [health information] technology," which may take EHRs offline or may degrade an EHRs' performance for a short time, Correa said.

5. **Infeasibility exception**: Actors are protected when they deny access, exchange or use of EHI due to the infeasibility of the situation, such as technology limitations or uncontrollable events. "Maybe an individual requests EHI in a certain format that you are not able to provide," she said.

6. **Content and manner**: This exception allows actors to limit and alter how EHI is provided. "It must be provided in a manner [the] requestor asks for unless you're unable to fill the request and you can't reach agreeable terms with the requester," she said.

7. **Fees**: Actors are permitted to charge fees for access, exchange and use of EHI, but they must be cost-based and nondiscriminatory.

8. **Licensing**: Access may be blocked because the actor is in the middle of licensing health information technology.

Enforcement Rule for Providers Is TBD

What happens if providers, HIT developers and health information exchanges (HIEs) block information in violation of the regulation? There are several answers. So far, the HHS Office of Inspector General (OIG) on April 24 proposed an enforcement regulation for HIT developers and HIEs, with penalties up to $1 million.[4] That includes providers if they're hosting or facilitating an information exchange among other providers, Greene said.

There's no proposed enforcement rule for providers yet, and it's anyone's guess which agency will take that on—CMS, the HHS Office for Civil Rights or OIG. How providers will be dinged for information also is unknown. The statute said there should be appropriate "disincentives using existing authorities," Greene said. "It's not clear what existing authorities would apply to providers," but all will be revealed when the enforcement rule comes out.

Contact Greene at adamgreene@dwt.com and Correa at lyracorrea@dwt.com.

1 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642 (May 1, 2020) , https://bit.ly/32vJ6RI.
2 Adam Greene and Lyra Correa, "Identifying and Remediating Information Blocking Practices," webinar, Health Care Compliance Association, October 15, 2020, https://bit.ly/3e7IzZX.
3 Nina Youngstrom, "Checklist for Compliance With Information-Blocking Rule," *Report on Medicare Compliance* 29, no. 39 (November 2, 2020).
4 Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules, 85 Fed. Reg. 22,979 (April 24, 2020) , https://bit.ly/3el1hM9.