

Health Information Compliance Alert

Interoperability: Final Rule Lays Out Data Blocking Exceptions

Understand the conditions, objectives, and categories.

There's no denying that data sharing between providers helps improve delivery of care and coordination between organizations and specialists. In the past, definitions of what constituted information blocking were complicated and created confusion in the industry, but a recent rule offers practitioners new standards and clearcut parameters.

Details: Just as COVID-19 and the public health emergency (PHE) were ramping up in the U.S., the **HHS Office of the National Coordinator for Health Information Technology** (ONC) and the **Centers for Medicare & Medicaid Services** (CMS) issued a pair of "transformative" final rules to address interoperability and patients' access to their health data. The long-awaited policies - published in the Federal Register on May 1 - are a follow-up to last year's proposals to act on provisions in the 21st Century Cures Act (See Health Information Compliance Alert, Vol. 19, Nos. 2 & 3).

"From the start of our efforts to put patients and value at the center of our healthcare system, we've been clear: Patients should have control of their records, period. Now that's becoming a reality," said HHS Secretary **Alex M. Azar** in a release. "These rules are the start of a new chapter in how patients experience American healthcare, opening up countless new opportunities for them to improve their own health, find the providers that meet their needs, and drive quality through greater coordination," Azar stressed.

Updates Focus on Patient Access

Over the past couple of years, the feds have focused on a central theme in their health IT policy making: Patients, not clinicians or organizations, should have control of patients' health information. In both the ONC and CMS final rules, the agencies offer a mix of guidance and technology standards aimed at improving that primary goal; moreover, the feds want to ensure that providers and their business associates (BAs) don't block patients from getting their records in the future.

"The new rules also prohibit certain 'information blocking' by providers, health information exchanges and networks, and IT developers," explains New York-based attorney **Ada Kozicz** with **Rivkin Radler LLP** in online analysis.

Kozicz continues, "Practices that restrict access, exchange or use of electronic health information are considered anti-competitive and will not be permitted."

See ONC's Data Sharing Specifics

According to ONC, "actors" will have eight exceptions to the information blocking rule that will fall under two distinct categories. More importantly, these actors must make "reasonable" attempts to eliminate "harm" while securely transmitting data to other entities and offering patients safe access to their electronic health information (EHI), ONC advises.

Definition: In order to determine if this applies to your organization, consider this definition of what the ONC calls an "actor." In broad terms, ONC final rule guidance organizes "actors" into three groups: healthcare providers; health IT developers; and health information networks (HINs) or health information exchanges (HIEs). See detailed federal descriptions at www.healthit.gov/cures/sites/default/files/cures/2020-03/InformationBlockingActors.pdf.

Categories: ONC splits the eight data blocking exceptions into two categories. Five of the exceptions "involve not fulfilling requests to access, exchange, or use EHI" and the other three concern "procedures for fulfilling requests to access, exchange, or use EHI," a fact sheet indicates.

Here is a short overview of the eight information blocking exceptions outlined in the ONC fact sheet on the Cures Act, including a breakdown by category:

Exceptions that fall under the "not fulfilling" requests category:

1. Preventing harm: Under this exception, actors "engage in practices that are reasonable and necessary" to protect the public and patients from harm; therefore, not sharing patient data might be justified to prevent harm under certain conditions. This exception carries a list of four conditions that include preventing harm and scope of practice.

2. Privacy: Actors might not share information to safeguard patients' privacy and also to align with state and federal privacy laws like the HIPAA Privacy Rule. This exception requires actors to meet at least one of four conditions in its sub-exceptions' list with a focus on specific provisions under the HIPAA rules.

3. Security: In this scenario, actors might "interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met," the fact sheet suggests. There are three key conditions on security exceptions - including subjects like protecting the integrity of the EHI and ensuring non-discriminatory practices.

4. Infeasibility: Occasionally, actors lack the necessary technological tools and legal rights to allow the use, access, or exchange of data, making it impossible for them to complete an individual's request for EHI. There are three strict conditions - uncontrollable events, segmentation of data, and infeasible circumstances - under this exception, but actors must only meet one of them. Additionally, actors must send a written explanation to requestors within 10 days of the request letting them know why they cannot fulfill the requests.

5. Health IT performance: Sometimes it's necessary for IT staff to do maintenance, upgrades, and updates to ensure that software and hardware run smoothly. During those downtimes, information blocking is OK because the IT work is necessary to improve interoperability. This exception covers two separate sets of conditions:

- The first group of three conditions deals with health IT implementation and timelines.
- The second set focuses on the actor's business relationship with third-party vendors, apps, and negative impacts.

Exceptions that fall under the procedures for fulfilling requests category:

6. Content & manner: This exception clarifies the minimum actors must include in the EHI content as well as the manner in which they deliver the data. Content and manner conditions are as follows:

- According to the content conditions, actors can use the United States Core Data for Interoperability (USCDI) standards for up to 24 months after the Cures Act final rule publication date as an EHI guide; however, after the 24-month period ends, actors must use Cures Act guidelines.
- The manner conditions relate that alternative means of EHI transfer are sometimes necessary, and actors must comply with stipulations accordingly.

7. Fees: Under this exception, actors can charge fees for the access, exchange, or use of EHI, but they cannot be "opportunistic" or "exclusionary." There are three required fee conditions. They include:

- The basic conditions suggest that actors' fees must be fair and uniformly applied to all requestors, related to actual costs of EHI transfers, and not created to compete with other actors.
- Exception exclusions may occur when a patient or the patient's representative requests EHI electronically or through health IT.
- Fees must comply with EHI certification requirements.

8. Licensing: Actors have the right "to protect the value of their innovations and charge reasonable royalties in order to earn returns on the investments they have made to develop, maintain, and update those innovations," the fact sheet says. The three conditions under this exception point to licensing negotiations and timelines, parameters of the license, and other interoperability provisions.

Bottom line: Compliance with the information blocking rules is required by Nov. 2, 2020, which doesn't leave actors

much time to update their EHI request policies and align them with new federal regulations.

"It remains unclear whether regulators enforcing the information blocking rules will generously interpret good-faith efforts to comply or stringently second-guess determinations with the benefit of hindsight," warn attorneys **Olivia Seraphim, Nesrin Garan Tift, and Elizabeth S. Warren** with **Bass, Berry & Sims PLC** in online analysis. "Taking proactive steps now to address the requirements of the rules, including documenting processes to promote meeting exceptions and training employees on new and revised policies, should pay dividends as compliance with the rules becomes mandatory," they advise.

On a COVID-19 related note, ONC has issued an enforcement discretion and will tack on three months from the compliance deadline before it starts enforcing the rules, which is a positive for struggling practices.

Stay tuned: Health Information Compliance Alert will continue analyzing different facets and provisions of the ONC and CMS final rules in future issues.

Resources: Find the ONC rule at

<https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification> and review the CMS rule at www.federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and.