COSMOS
Navigate the Compliance Universe

Compliance Today - September 2020
The impact of the final ONC and CMS interoperability rules on health information

By Michaela Andrawis, Lyra Correa, and Miriam Ricanne Swedlow

Michaela Andrawis (michaelaandrawis@dwt.com) is an Associate in the Los Angeles office, **Lyra Correa** (lyracorrea@dwt.com) is an Associate in the Washington, DC, office, and **Miriam Ricanne Swedlow** (miriamswedlow@dwt.com) is an Associate in the Seattle office of Davis Wright Tremaine LLP.

- linkedin.com/in/michaela-andrawis-247ba77
- linkedin.com/in/lyra-correa-73a245160
- linkedin.com/in/miriam-ricanne-swedlow-572005ba

On March 9, 2020, the U.S. Department of Health & Human Services (HHS), through the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS), published separate, but related, final rules implementing the interoperability and patient access provisions of the 21st Century Cures Act (Cures Act).[1] The earliest compliance date for the rules is November 2, 2020,[2] and healthcare entities will find that there is a lot to do between now and then.

The ONC Rule[3] focuses on significant changes to the ONC's existing health information technology (IT) certification program, addresses "information blocking," and carves out eight categories of "reasonable and necessary" practices that will not constitute information blocking. The CMS Rule[4] addresses many of the same patient access and interoperability issues as the ONC Rule, but it applies to Medicare, Medicare Advantage, Medicaid, Children's Health Insurance Program, and Qualified Health Plan issuers on federally facilitated exchanges.

These rules will significantly affect healthcare providers, health plans, health IT vendors, and patients in the years ahead. Once implemented:

- **Healthcare providers and health IT companies** will risk potential penalties or disincentives for intentionally or inadvertently engaging in information blocking.
- **Hospitals** will be required to make reasonable efforts to send real-time electronic patient event notifications to certain other healthcare providers and their business associates (under new Medicare conditions of participation).
- **Health IT companies** adapting new application programming interface (API) standards to give third-party applications access to electronic health information will still have to comply with federal and state privacy and security requirements, such as Health Insurance Portability and Accountability Act (HIPAA), the Federal Trade Commission Act, the California Confidentiality of Medical Information Act, the Texas Medical Records Privacy Act, and others.
- **Patients and health plan members** will have greater automated access to their health information through

third-party apps, regardless of how well they understand the potential benefits or risks.

For some, these regulations mark a watershed moment in consumers' access to their health information, potentially enabling unprecedented health IT innovation. For others, these rules present both an immediate danger to patient privacy by funneling health data outside of the protections of HIPAA and into a perceived privacy Wild West and a potentially murky intrusion into current commercial contracting practices related to health information sharing.

Regardless, the rules create new compliance risks and hurdles for health providers, health plans, and health IT vendors. This article highlights some of the compliance considerations and impacts of the new regulations on information sharing, care coordination through real-time e-notifications, and certified APIs.

Compliance considerations for information blocking

The following section highlights key questions and considerations related to the ONC Rule's information-blocking regulations and describes potential next steps for complying with the new rules.

Do the information-blocking regulations apply to my organization?

The ONC Rule's information-blocking regulations apply to three categories of actors:

- Healthcare providers (e.g., healthcare facilities, laboratories, pharmacies, physicians),
- Health information networks, and
- Health IT developers of *certified* health IT.

The category an entity fits into may change depending on if the entity provides certified information technology or a data platform that enables the access, exchange, or use of electronic health information (EHI) by others. The actor category an entity fits into when engaging in a practice will affect its risk exposure to enforcement under the information-blocking regulations.

What do the information-blocking regulations prohibit?

Predictably, the information-blocking regulations prohibit information blocking, which is broadly defined by the Cures Act as a practice that, except as required by law or specified by the HHS as a reasonable and necessary activity, is "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information."[5]

Both the Cures Act and ONC Rule provide examples of practices that constitute information blocking, including:

- Imposing formal or informal restrictions on access, exchange, or use of EHI;
- Implementing health information technology in ways that are likely to restrict the access, exchange, or use of EHI with respect to exporting complete information sets or in transitioning between health information technology systems;
- Discouraging efforts to develop or use interoperable technologies or services by exercising influence over customers, users, or other persons;[6]
- Discrimination that frustrates or discourages efforts to enable interoperability; and

- Rent-seeking and opportunistic pricing practices that make information sharing cost prohibitive.[7]

Do the information-blocking regulations apply to all information?

No! The information-blocking regulations only apply to EHI, defined as electronic protected health information (ePHI) under HIPAA, to the extent that the ePHI would be included in a designated record set *regardless* of whether the records were used or maintained by or for a HIPAA-covered entity.

Any health information not included in EHI is not required to be shared, and any practice related to data outside of EHI is not information blocking. However, through May 2, 2022, information-blocking enforcement is further limited to information data elements within the United States Core Data for Interoperability (USCDI) standard.[8]

Other exemptions to the information-blocking regulations include:

- Practices that are required by law (e.g., local, state, federal) and
- Practices that are specified by HHS as reasonable and necessary (i.e., the regulatory exceptions).

Does an information-blocking exception apply?

The Cures Act authorizes HHS to identify reasonable and necessary activities that do*not* constitute information blocking. The ONC Rule therefore lists eight categories of exempt practices, each with specific conditions.[9] Each practice that meets the conditions of at least one exception will not be treated as information blocking.

If a practice does not meet all of the conditions of an exception, it will not automatically constitute information blocking. However, such practices will not have guaranteed protection from civil monetary penalties or appropriate disincentives and will be evaluated on a case-by-case basis to determine whether information blocking has occurred (e.g., whether the practice rises to the level of an interference and whether the actor acted with the requisite intent).

Accordingly, actors are encouraged to fully align their current business practices with respect to access, exchange, or use of EHI, with one of the following HHS-recognized exceptions, or as close as reasonably possible (see Table 1).

Exceptions that involve not fulfilling requests to access, exchange, or use EHI	
1. Preventing harm exception	Practices that are likely to interfere with access, exchange, or use of EHI may be justified if the practices are reasonable and necessary to prevent harm to a patient or another person.
2. Privacy exception	An actor does not have to fulfill a request to access, exchange, or use EHI in a way that is prohibited under state or federal privacy laws.

3. Security exception	Practices that are likely to interfere with access, exchange, or use of EHI may be justified in order to safeguard EHI when the practice is tailored to specific security risks and implemented consistently in a nondiscriminatory manner.
4. Infeasibility exception	Legitimate practical challenges may limit an actor's ability to comply with requests for access, exchange, or use of EHI (e.g., lack of technological capabilities, legal restrictions outside actor's control).
5. Health IT performance exception	Reasonable and necessary practices that temporarily make health IT unavailable or that degrade the health IT's performance may be permitted for regular maintenance or improvement of the overall performance of the health IT.
Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI	
6. Content and manner exception	An actor may be permitted to limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided the content and manner conditions are met.
7. Fees exception	Actors may charge fees, including fees that result in a reasonable profit margin, related to the development/provision of technologies and services that enhance interoperability while not protecting opportunistic fees and discriminatory practices that interfere with access, exchange, or use of EHI.
8. Licensing exception	Protects the value of actors' innovations and allows the charge of reasonable royalties to earn returns on investments made to develop, maintain, and update those innovations.

Table 1: Exceptions to the information-blocking definition

What are the enforcement provisions?

The potential penalties and disincentives for information blocking under the Cures Act depend, in part, on the violating actor and nature of the transgression.

- **Health IT developers and health information networks** can be subject to civil monetary penalties of up to $1,000,000 per violation for all identified violations.[10] Per the Office of Inspector General, the penalty determination will take into account the "nature and extent of the information blocking and harm resulting from such" action (e.g., number of patients and/or providers affected, the number of days the information blocking persisted).
- **Healthcare providers** will be referred to the appropriate agency and subjected to appropriate disincentives

using authorities under applicable federal law, as the HHS sets forth through notice and comment rulemaking.

- **CMS-regulated clinicians and hospitals** must submit self-attestations to certain Promoting Interoperability Program requirements.[11] "Beginning in late 2020, and starting with data collected for the 2019 performance year data, CMS will publicly report eligible [clinicians and hospitals] that may be information blocking based on" these self-attestations.