NOW + NEXT

HEALTH CARE ALERT | NIXON PEABODY LLP

MARCH 11, 2020

Long-awaited CMS and ONC final rules on interoperability, patient access and information blocking released

By Laurie Cohen, Rebecca Simone, Valerie Breslin Montague, Caitlin Donovan, Jacalyn Smith and Meredith LaMaster

On March 9, 2020, the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) issued final rules implementing Title IV of the 21st Century Cures Act (the "Cures Act") and Executive Order 13813. The final rules are intended to promote interoperability and support the access, exchange, and use of electronic health information (EHI). The rules also are intended to reduce burdens and costs related to accessing EHI and to reduce occurrences of information blocking.

The CMS final rule

The CMS final rule outlines a number of policies to regulate Medicare Advantage ("MA") organizations, Medicaid, CHIP, and Qualified Health Plan issuers on the Federally-Facilitated Exchanges. The rules require these organizations to implement and maintain a Patient Access Application Programming Interface (API) that allows patients to access certain portions of their clinical information, claims data, and encounter information through an app chosen by the patient. The CMS final rule also requires MA organizations, Medicaid Fee-for-Service (FFS) programs, Medicaid managed care plans, CHIP FFS programs, and CHIP managed care plans (collectively "CMS Regulated Payors") to implement a Provider Directory API, allowing patients to use their chosen app to access provider directory information to help determine "in network" providers. The Patient Access API and the Provider Directory API must be implemented by January 1, 2021.

The CMS final rule also requires CMS Regulated Payors to electronically exchange certain clinical data at the request of the patient. This requirement takes effect on January 1, 2022.

The ONC Final Rule

Who is affected by the final rule? The ONC final rule focuses on four types of actors: (1) providers; (2) health IT developers; (3) health information networks (HINs); and (4) health information exchanges (HIEs), (collectively, the "Actors"). However, it also impacts any person, provider, or corporation that accesses, exchanges, or transfers EHI.

- Providers. Health care providers under the ONC final rule include all health care providers in Section 3000 of the Public Health Service Act, which broadly references health care facilities and clinicians of all types.
- Health IT Developers. Health IT Developers include any individual or entity that offers or creates Certified Health IT. Certified Health IT means technology that is certified under the ONC's program for voluntary certification for health information technology.
- Health Information Networks and Health Information Exchanges. Under the final rule, HINs and HIEs have been consolidated under a single definition. To qualify as an HIN or HIE, an entity must determine, control, or administer any requirement, policy, or agreement that permits, enables, or requires the use of technology or services for access, exchange, or use of EHI for more than two unaffiliated individuals or entities.

What constitutes EHI?

EHI includes electronic protected health information (ePHI), as defined in HIPAA, to the extent the ePHI is maintained in a HIPAA designated record set. Note that the records do not have to be used or maintained by or for a HIPAA covered entity to fall within the definition of EHI. Until 24 months after the ONC rule's publication date, for purposes of the information blocking definition, EHI is limited to those data elements in the United States Core Data for Interoperability (USCDI) standard set forth in the ONC final rule

What is information blocking?

The Cures Act defines information blocking as a practice performed by the Actors that is apt to interfere with, preclude, or substantially hinder access, exchange, or use of EHI. Actors may not engage in prohibited information blocking or other actions that inhibit allowable exchange, access, and use of EHI.

What are the exceptions to the prohibition on information blocking?

Recognizing the importance of protecting patient safety and promoting the privacy and security of EHI, the ONC Final Rule includes several exceptions to the prohibition of information blocking including:

1. **Preventing Harm Exception—**When an Actor's practice is likely to interfere with the access, exchange, or use of EHI in order to prevent harm, the practice may not be considered information blocking. Four key conditions of the exception must be met: (1) the Actor must reasonably believe that the practice will materially reduce a risk of harm; (2) the Actor's practice may not be overly broad; (3) the Actor's practice must meet a condition from each of these categories: type of risk, type of harm, and implementation basis; and (4) the practice must allow the patient a right to request an individualized determination of risk of harm.

2. **Privacy Exception**—When an Actor's practice of not fulfilling a request to access, exchange, or use EHI is done in order to protect an individual's privacy, the practice is not considered information blocking. At least one of four sub-exceptions must be met to satisfy this exception: (1) a precondition is not satisfied, (2) a Health IT Developer of certified health IT is not covered by HIPAA, (3) an individual's request for EHI is denied consistent with certain HIPAA Privacy Rule provisions, or (4) the Actor is respecting an individual's request not to share information.

3. **Security Exception**—When an Actor's practice is likely to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, the practice will not be deemed information blocking. The conditions of this exception are that the practice has to be: (1) directly correlated to safeguarding the confidentiality, integrity, and availability of EHI; (2) tailored to specific security threats; and (3) implemented in a consistent, non-discriminatory manner. Additionally, the practice must rely on a qualifying organizational security policy or a qualifying security determination.

4. **Infeasibility Exception**—When an Actor's practice of not fulfilling a request to access, exchange, or use EHI is due to the infeasibility of the request, it does not qualify as information blocking. Infeasible events include: (1) uncontrollable events; (2) segmentation, where the Actor does not have the ability to unambiguously segment the EHI that is requested; or (3) infeasibility under the circumstances. Actors have 10 business days from their receipt of a request to provide a written response as to why a request is infeasible.

5. **Health IT Performance Exception**—When an Actor's practice is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of EHI, that practice is not information blocking. To meet this exception, the practice must: (1) be enacted for only as long as is reasonably necessary to maintain or improve the performance of the health IT; (2) be enacted in a consistent, non-discriminatory manner; and (3) meet required guidelines if unavailability is initiated by a Health IT Developer of certified health IT, an HIE, or an HIN.

6. **Content and Manner Exceptions**—When the content and manner of an Actor's practice is a response to a request for EHI, that practice is not deemed information blocking.

7. **Fees Exception**—When an Actor's practice is charging fees for accessing, exchanging, or using EHI, that practice does not constitute information blocking. To meet this exception, a practice must meet the basis for fees condition, not be specifically excluded, and comply with Conditions of Certification in Section 170.402(a)(4).

8. **Licensing Exception**—When an Actor's practice is to license interoperability elements in order for EHI to be accessed, exchanged, or used, that practice is not information blocking. To satisfy the exception, the Actor must begin license negotiations within 10 business days from the request date and negotiate a license within 30 days of the request date, among other conditions.

Failure to fall within one of these enumerated exceptions is not fatal and does not automatically subject the Actor to penalties. Rather, an Actor's practice will be assessed on a case-by-case basis to determine whether there was impermissible information blocking and interference with EHI records.

How does the ONC final rule impact the Health IT Certification Program?

The final rule also impacts the ONC Health IT Certification Program. The Health IT Certification Program creates a set of standards for health IT software platforms, particularly APIs.

Certification Requirements. Certification now requires that APIs provide access to all data elements of a patient's record without additional burdens. Third-party applications must register

with an authorized server. ONC established that the review process for third-party applications cannot not violate the information blocking rules. Certified Health IT Developers cannot institute any vetting process for applications that are facilitating patient access to EHI.

Real World Testing. Health IT Developers that create Health IT Modules must certify that one or more of the certification criteria focused on interoperability and data exchange or availability has been met. Every Developer must create real world testing plans. Developers must submit a metric for each certification criteria that applies to their modules. They must also work with the ONC-Authorized Certification Bodies (ONC-ACB) to determine when the testing plans must be submitted. Health IT developers are required to publish the testing plan by December 15 of each year.

Condition of Certification. The final rule also impacts how Health IT Developers can communicate about specific information. Health IT Developers cannot restrict communication related to the usability, interoperability, and security of health information technology. Health IT Developers cannot restrict communications about patients' experience using APIs or other third-party applications. They cannot prohibit communication about the business practices of Health IT Developers.

When does the ONC final rule take effect?

Portions of the ONC final rule become effective 60 days after publication, including certain communication restrictions on Health IT Developers. Recognizing that compliance takes time, many of the provisions have delayed implementation dates. For instance, compliance with the information blocking provisions is required six months from the date of publication of the ONC final rule. Real-world testing plans are due on December 15, 2020.

More to come

To follow this initial overview of the newly-released CMS and ONC final rules, our Nixon Peabody health care team intends to publish more in-depth guidance on the nuances of these regulations for health care facilities, clinicians, and Health IT Developers.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Laurie T. Cohen at lauriecohen@nixonepeabody.com or 518-427-2708
- Rebecca Simone at rsimone@nixonpeabody.com or 516-832-7524
- Valerie Breslin Montague at vbmontague@nixonpeabody.com or 312-977-4485
- Caitlin A. Donovan at cdonovan@nixonpeabody.com or 518-427-2737