# CMS and ONC Finalize Interoperability and Information Blocking Rules

Insights 03.18.20

**PROFESSIONAL**

**ANDREA FREY**
Partner
**San Francisco**
**San Diego**

**MONICA MASSARO**
Director, Government Relations & Public Policy
**Washington, D.C.**

**MARTIN A. CORRY**
Co-Chair of Government Relations & Public Policy Department
**Washington, D.C.**

On March 9, 2020 the U.S. Department of Health and Human Services released long-awaited final rules governing interoperability, information blocking, and patient access, over a year after proposed rules were issued. These final rules, issued by the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS), were the subject of debate over the past year, and embody the most extensive health care data sharing policies put forward by the federal government to date. They are awaiting publication in the Federal Register.

The lack of seamless data exchange in health care as a result of data silos often results in fragmented care, which can lead to poor health outcomes and drive up costs. The final rules (CMS's final rule is available here, and ONC's final rule is available here) aim to break down these barriers to enable better patient access to and sharing of health information, while also improving interoperability and spurring the development of new technology. A summary of the key provisions follows.

**Public Reporting and Information Blocking:** The final CMS rule builds on information blocking provisions introduced under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA). MACRA requires clinicians, hospitals and critical access hospitals seeking meaningful use incentive payments to demonstrate they have not knowingly and willfully restricted the compatibility or interoperability of certified EHR technology (CEHRT). To implement these interoperability requirements, CMS adopted three attestations that providers must make regarding their use of CEHRT: that they did not knowingly and willfully restrict compatibility or interoperability of CEHRT; that they took steps to ensure that CEHRT was connected, compliant with relevant standards, allowed timely access by patients, and allowed timely and secure exchange of electronic health information; and that they responded in good faith and timely to requests to retrieve or exchange electronic health information. The final rule adopts the proposal in the proposed rule to publish the responses of clinicians, hospitals and critical access hospitals (CAHs) to these attestations. To implement this rule, CMS will add a new indicator on Physician Compare for clinicians and medical groups that respond "no" to any of the attestations, and CMS will post the names of hospitals and CAHs that do the same on a website. This information will be posted beginning in late 2020 for the 2019 reporting period.

In December 2016, section 4004 of the 21st Century Cures Act added section 3022 of the Public Health Service Act (PHSA), which prohibits "information blocking" by health care providers, health IT developers, and health information exchanges. The PHSA defines information blocking as a practice by a health care provider, health IT developer or health information exchange or network that is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information. A health care provider is guilty of information blocking only if it knows that its practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

The PHSA also requires the Secretary of HHS to identify reasonable and necessary activities that do not constitute information blocking for purposes of the PHSA. In its final rule, ONC creates eight exceptions to the information blocking prohibition. Each of the exceptions has detailed requirements. To be eligible for an exception, a practice must meet all of the requirements of the exception. However, the failure to meet an exception does not mean that a practice constitutes information blocking; it just means that the practice does not have guaranteed protection, and would be open to evaluation on the facts. There are exceptions for:

- Practices intended to reduce the risk of harm to a patient or another person (this exception accommodates the HIPAA provisions that allow a covered entity to deny an individual access to health information);
- Practices intended to protect an individual's privacy;
- Practices intended to protect the security of electronic health information;
- Not fulfilling a request to access health information because the request is infeasible;
- Practices intended to maintain or improve the performance of information technology;
- Limiting the content of a response to a request for health information where the provider is technically unable to fulfill the request or cannot reach agreeable terms with the requester;
- Charging uniform, reasonable, cost-based fees for accessing or providing health information (but the exception does not cover fees charged for the electronic access to an individual's electronic health information by the individual, the individual's personal representative, or someone designated by the individual); and
- Reasonable practices relating to licensing interoperability technology (this exception has particular requirements for the negotiation and content of licenses and would be of interest to both developers and users of interoperable technology).

**Digital Contact Information:** As part of the 21st Century Cures Act, Congress required the Secretary of the U.S. Department of Health and Human Services to create a provider digital contact information index. This index is publicly available as part of the National Plan and Provider Enumeration System (NPPES). In the second half of 2020, CMS will begin publicly reporting providers who do not list or update their digital contact information in the NPPES. The goal of this requirement is to encourage providers to make this information easily accessible, to facilitate care coordination and data exchange, and ultimately to increase the number of providers sharing how to securely transmit electronic information to the provider. CMS may consider incentive-based approaches or other enforcement mechanisms to further promote this goal in the future.

**Admission, Discharge, and Transfer Event Notifications:** Effective six months after publication of the CMS's final rule, the Medicare Conditions of Participation (CoPs) for hospitals, including psychiatric hospitals and critical access hospitals, will include a requirement to send electronic patient event notifications of a patient's registration in an emergency department, admission as an inpatient, discharge, or transfer to another healthcare facility, community provider, or practitioner, unless this notification is inconsistent with a patient's expressed privacy preferences. In particular, if a hospital utilizes an electronic medical record system or other electronic administrative system which conforms with the content exchange standard at 45 C.F.R. § 170.205, the notification capacity must be operational, including notification of at least the patient name, treating practitioner name, and sending institution name. In addition, when sending a notification to a post-acute provider or supplier or other practitioner or health care provider for treatment, care coordination, or quality improvement, the hospital must make a reasonable effort to include the patient's primary care practitioner, that practitioner's practice group or entity, or other practitioner or entity identified by the patient as primarily responsible for the patient's care. See 42 C.F.R. § 482.24 (conditions of participation; medical record services); 42 C.F.R. § 482.61 (applicable to psychiatric hospitals); 42 C.F.R. § 482.638 (applicable to critical access hospitals).

**Patient Access APIs:** By January 1, 2021, CMS-regulated payers (including Medicare Advantage organizations, Medicaid and CHIP fee for service programs, Medicaid managed care plans, and CHIP managed care entities) will be required to implement and maintain a secure, standards-based (HL7 FHIR Release 4.0.1) application programming interface, or API, that allows patients to easily access their claims and encounter information, including cost, as well as a defined sub-set of their clinical information through third-party applications of their choice. The Patient Access API must, at a minimum, make available

adjudicated claims (including provider remittances and enrollee cost-sharing); encounters with capitated providers; and clinical data, including laboratory results (when maintained by the affected payer). Data must be made available no later than one business day after a claim is adjudicated or encounter data is received. Payers are required to provide specified data they maintain with a date of service on or after January 1, 2016. The rule is intended to facilitate the creation and maintenance of a patient's cumulative health record with their current payer.

**Provider Directory APIs:** By January 1, 2021, CMS-regulated payers will also be required to make provider directory information publicly available via a standards-based API. (Qualified Health Plan issuers on the federal exchanges are already required to make provider directory information available in a specified, machine-readable format.) Specifically, CMS is requiring that the provider directory API be accessible via a public-facing digital endpoint on a payer's website to ensure public discovery and access. At a minimum, the provider directory API must contain provider names, addresses, phone numbers, and specialties. For MA organizations that offer MA-PD plans, they must also make available pharmacy directory data, including the pharmacy name, address, phone number, number of pharmacies in the network, and mix (specifically the type of pharmacy, such as a retail pharmacy). All directory information must be made available to current and prospective enrollees and the public through the provider directory API within thirty (30) days of a payer receiving provider directory information or an update to the provider directory information.

CMS hopes that making provider directory information broadly available to the public will encourage innovation by allowing third-party application developers to create services that help patients find providers for care and treatment, as well as help clinicians find other providers for care coordination. Making this information more widely accessible may also improve the quality, accuracy, and timeliness of this information.

**Payer-to-Payer Data Exchange:** Beginning January 1, 2022, CMS-regulated payers (as described above, including QHPs on federal exchanges) will be required to implement a process to exchange certain patient clinical data (specifically the U.S. Core Data for Interoperability (USCDI) version 1 data set) with a date of service on or after January 1, 2016 at a current or former enrollee patient's request, allowing patients to take their information with them as they move from payer to payer over time to help create a cumulative health record with their current payer. Given payers' unique position to provide patients with a comprehensive picture of their claims and encounter data, CMS believes that the payer-to-payer data exchange will empower patients to make more meaningfully-informed decisions about their care and coverage, while also more effectively coordinating care and reducing costs. In an effort to reduce the burden on payers, CMS also finalized a provision that a payer is only obligated to share data received from another payer in the electronic form and format it was received.

*For more information, please contact Paul Smith or Andrea Frey in San Francisco, Amy Joseph or Jeremy Sherer in Boston, Marty Corry or Monica Massaro in Washington, D.C., or your regular Hooper, Lundy & Bookman contact.*