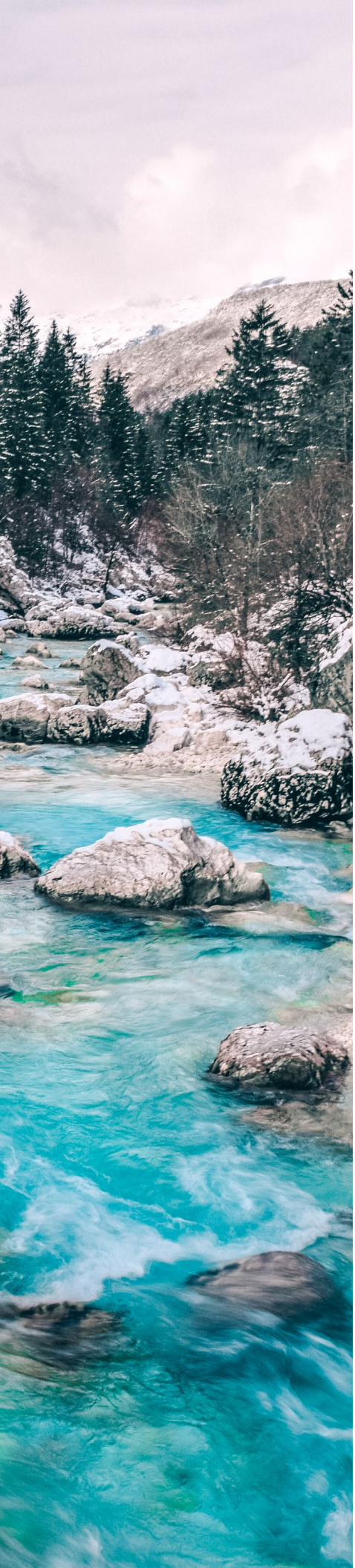
Two Federal Rules Implementing New Health Information Sharing Requirements and Implications for Health Care Providers

Updated April 24, 2020



On Monday, March 9, 2020, the U.S. Department of Health and Human Services (HHS) released two rules supporting interoperability and patient access provisions of the 21st Century Cures Act. The rules, issued by the HHS Office of the National Coordinator for Health Information Technology (ONC) and Centers for Medicare & Medicaid Services (CMS), are intended to support patient access to health data and digital data exchange. The rules are scheduled to be published in the Federal Register on May 1, 2020.

These rules have significant financial and operational implications across the health care ecosystem, particularly relating to electronic health record exchange. ONC's anticipated economic impact of the rule acknowledges the broad scope (over 400,000 providers) and impact (up to $1.6 billion in total cost, just to health care providers) of these changes. These rules represent a fundamental shift in how health care providers will need to approach health information management (HIM) – HIM departments are now expected to be the primary facilitators of health data exchange.

This paper focuses on how health care providers should be preparing to comply and educate their staff and patients about the new health information sharing requirements.

Summary

- **The ONC released the "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program."[1]**

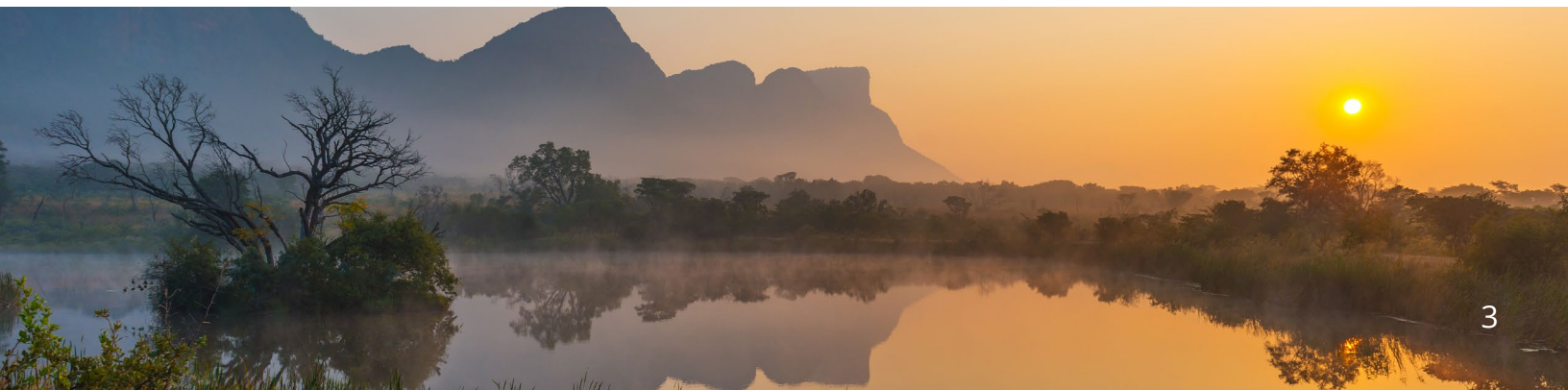
  - The ONC rule implements the 21st Century Cures Act prohibition on information blocking, including fines and financial disincentives, as well as exceptions to the broad information blocking prohibition. Providers will need to ensure readiness to comply 6 months after rule publication. This will likely require a detailed evaluation and refresh of all data request and sharing policies in addition to publicly documenting policies, to be prepared for any potential reports of information blocking.

- **CMS's "Interoperability and Patient Access"[2] final rule was released simultaneously with the ONC Rule.**

  - The CMS rule finalizes requirements for electronic notifications when a patient is admitted, discharged, or transferred. In addition, CMS reiterated the importance of the "Promoting Interoperability" attestations. Given these new statutory and regulatory definitions of information blocking, providers should be prepared to understand new actions they may have to take to respond affirmatively to the attestations.

- **In addition to these rules, the Administration announced its intention for further regulations governing interoperability for hospital providers as well as potential updates to HIPAA given the increased demand for and exchange of health data.**

[1] https://www.healthit.gov/cerus/sites/cerus/files/2020-03/ONC_Cures_Act_Final_Rule_03092020.pdf
[2] https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index



ONC Final Rule Overview

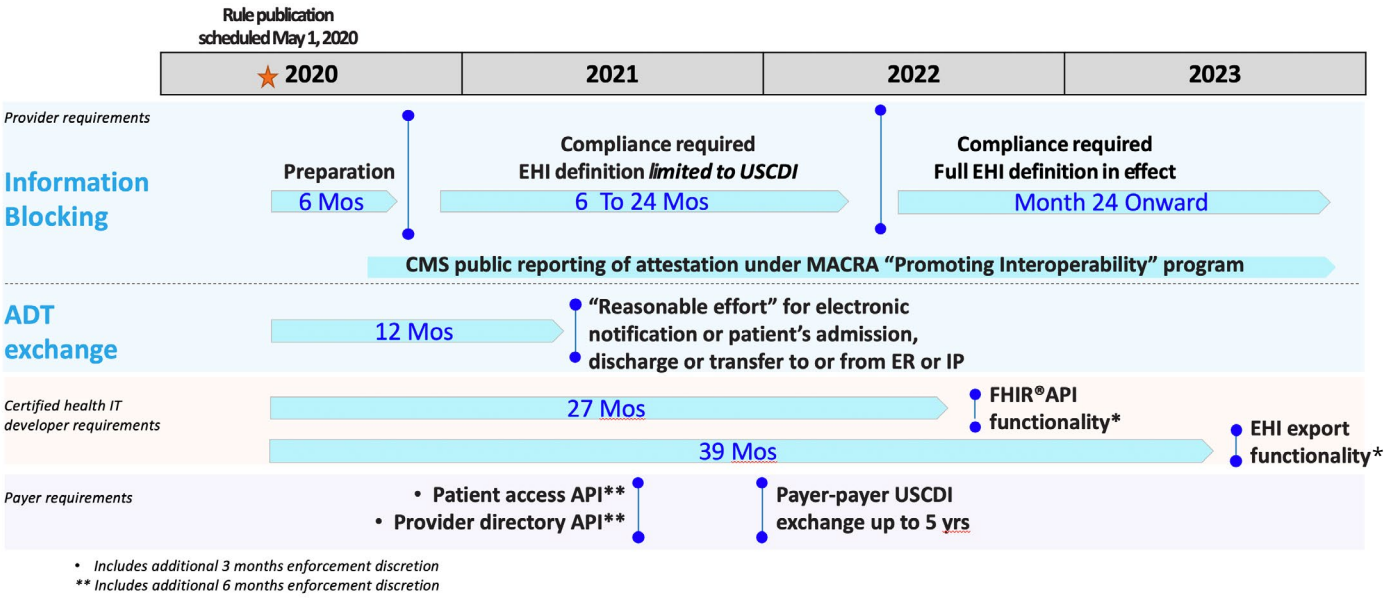
The ONC rule has three main areas of focus:

1. Updating ONC's health IT certification criteria,

2. Establishing conditions and maintenance required for health IT certification, and

3. Defining who is subject to the information blocking prohibition and eight (8) exception categories.

ONC's overall rule will go into effect 60 days after it is published in the *Federal Register*. More importantly, though, specific elements in the rule have effective dates tied to the date of the rule's publication (May 1, 2020). Detailed information about timing and the rule can be found in the following sections and in the ONC's fact sheets[3]. The below graphic includes a brief summary of key timelines for compliance.



[3]https://www.healthit.gov/curesrule/resources/fact-sheets

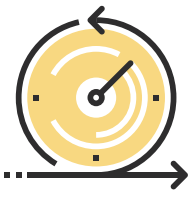
New Standards Advance Interoperability

The first two focus areas update the definition of certified electronic health record technology (CEHRT) and set conditions and maintenance of certification requirements for health IT developers. The rule sets new standards for application programming interfaces (APIs), including requiring data elements and use of a common interface, that advance interoperability by better facilitating electronic health information exchange.

New API standards: USCDI, HL7 FHIR

- **United States Core Data for Interoperability (USCDI)** becomes the standard for data exchange, replacing the Common Clinical Data Set (CCDS). Currently, the standard includes data elements such as clinical notes (as free text and unstructured data), certain patient demographic data (e.g., address, email, phone number), and other data categories (e.g., data provenance); however, the standard is intended to expand over time.

- **Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR)** is a common data sharing standard that defines how healthcare information, including clinical and administrative data, can be exchanged between different computer systems regardless of how it is stored in those systems. The current version of HL7 FHIR (Release 4.0.1) is required.



Timeline

Health IT developers need to update their certified health IT to support the USCDI for all certification criteria affected by this change within twenty-four (24) months after rule publication. However, in response to COVID-19 efforts, ONC announced an additional three (3) months of enforcement discretion.

Implications for Health Care Providers

While these requirements are largely the responsibility of developers of certified health IT to implement, providers should be familiar with the new USCDI standard and the use of FHIR, as other systems that interface with EHRs would benefit from these capabilities as well. In addition, as USCDI becomes relevant in determining information blocking, providers will need to understand how requests for clinical data map to USCDI.

Electronic Sharing Requirements Prevent Information Blocking

In addition to ensuring technology meets new certification requirements, providers must also prepare to comply with the "information blocking" prohibition and associated exceptions, which establish new requirements related to electronic information sharing.

Who is subject?

- **Health care providers** – The definition of "health care provider" in Section 3000 of the Public Health Service Act includes, amongst others, hospitals, ambulatory surgical centers, long term care facilities, health care clinics, community mental health centers, pharmacies, laboratories, physicians, and practitioners.

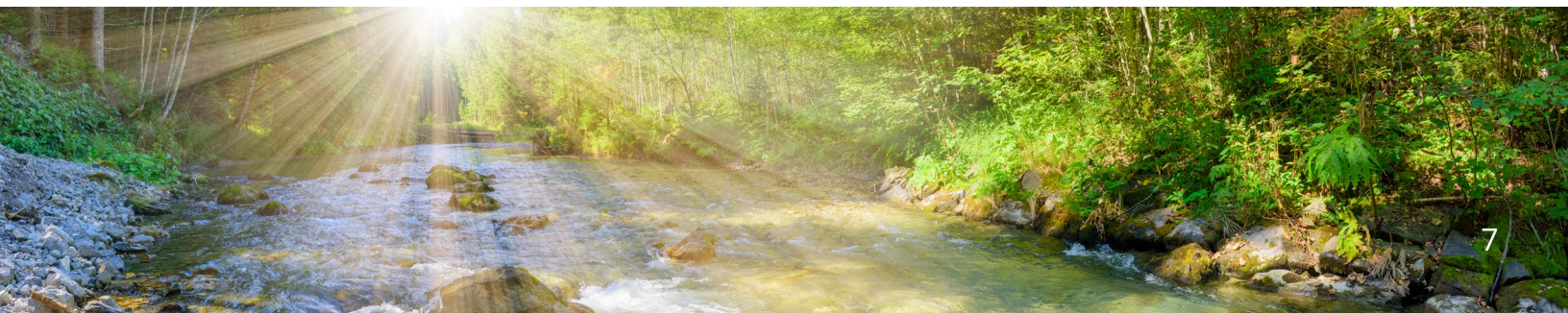
- **Health information networks or health information exchanges** – These entities administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI between more than two unaffiliated entities for treatment, payment, or health care operations purposes.

- **Health IT developers of certified health IT** – These entities develop or offer health information technology that is certified by ONC.

What is information blocking?

In the 21st Century Cures Act, Congress defined "information blocking" broadly as a **practice likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI)**. In the rule, ONC clarifies that EHI subject to information blocking restrictions generally includes data that is electronic protected health information (ePHI), as defined under HIPAA regulations. The caveat is that for the first 24 months after rule publication, EHI subject to information blocking will only refer to USCDI. Patient information that is de-identified is not considered EHI and is not protected.

For providers, the cost of non-compliance is "appropriate disincentives." For health information networks, health information exchange and health IT developers, the cost is financial penalties up to $1 million per instance.



What is not information blocking?

ONC identifies eight categories of reasonable and necessary activities that do not constitute information blocking, provided certain conditions are met. Referred to as exceptions, these categories of reasonable activities are intended to allow entities to conduct reasonable and necessary activities while still supporting seamless and secure access, exchange, and use of EHI.

The exception categories are further divided into two classes:

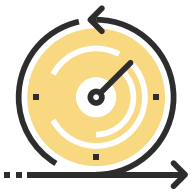
- Exceptions that involve not fulfilling requests to access, exchange, or use EHI
- Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI

Source: https://www.healthit.gov/curesrule/final-rule-policy/information-blocking

	Exception	Provided certain conditions are met, it is not considered information blocking if an actor:
1	Preventing Harm	Holds a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another person
2	Privacy	Believes use or disclosure of EHI is prohibited under state or federal privacy laws and meets at least one of four sub-exceptions
3	Security	Implements a qualifying organizational security policy or a qualifying security determination
4	Infeasibility	Meets one of three conditions – uncontrollable events, segmentation, infeasibility under circumstances – and the actor provides a written response to the requestor within 10 business days stating the reason for infeasibility
5	Health IT Performance	Makes health IT temporarily unavailable or degrades performance to benefit overall performance of the health IT
6	Content and Manner	Limits the content of its response or the manner in which it fulfills a request to access, exchange or use EHI provided certain conditions are met
7	Fees	Charges fees related to the development of technologies and provision of services that enhance interoperability
8	Licensing	Charges reasonable royalties to protect the value of their innovations and to earn returns on the investments they have made to develop, maintain, and update those innovations

NOT FULFILLING REQUESTS

PROCEDURES FOR FULFILLING REQUESTS



Timeline

All entities subject to the rule – health care providers, health information networks, health information exchanges and certified health IT developers - will have six months from rule publication to comply (i.e., by November 2, 2020)..

However, ONC states that enforcement of information blocking civil money penalties (CMP), which are relevant to entities other than health care providers, will not begin until established by future notice and comment rulemaking by the Office of the Inspector General (OIG). On April 22, the HHS Office of Inspector General (OIG) proposed a rule amending CMP regulations. Included in the rule are definitions of a violation of information blocking and factors considered when determining a penalty. The rule is currently open for comment and OIG would not begin enforcing CMPs for information blocking until the rule is effective.

Implications for Health Care Providers

In order to qualify as an exception to information blocking, entities must meet specific conditions under each of the categories listed above. It is likely that detailed analysis of each category's conditions and documentation of those conditions would be required to counter claims of information blocking.

As an example relevant for release of information (ROI), ONC detailed that the Fees Exception may apply (i.e., a provider may be able to charge a fee for access to clinical data and not be considered information blocking) if the fee meets multiple conditions:

- Two "basis for fees conditions," including four or more subcriteria for each condition
- Does not include any of four excluded fees
- Meets a condition where relevant

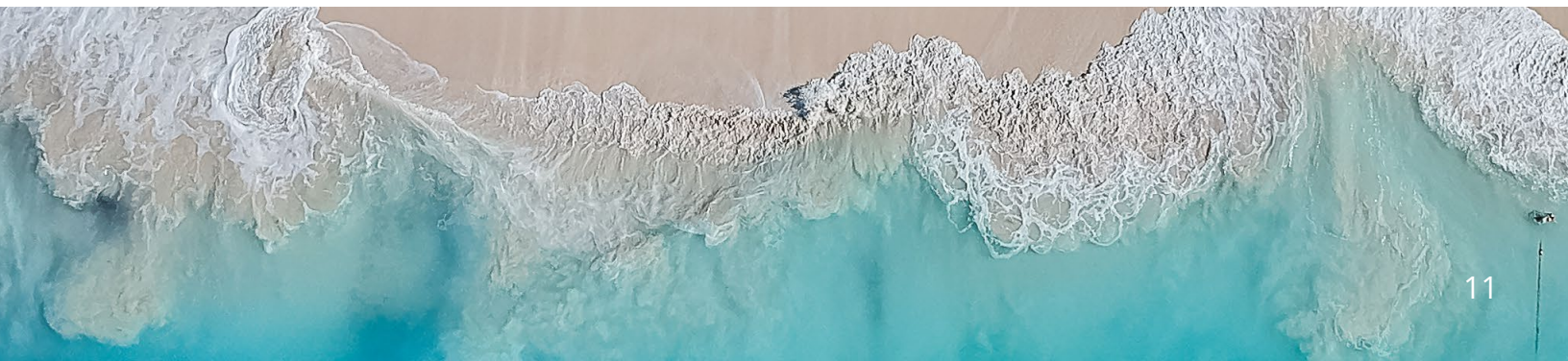
For each instance where a provider charges a fee, the provider would want to document that instance meets all of the above conditions.

ONC states that evaluation of information blocking complaints will be conducted on a case-by-case basis, which coupled with the complexity in the exception descriptions, suggests there are no "bright lines" on what does not constitute information blocking.[5] If a provider faces an information blocking complaint and believes its action falls under an exception to information blocking, the burden will be on the provider to share the context of the data request and prove its actions qualify as an information blocking exception.

Given the complexity of navigating the exceptions and proving that one is not information blocking, a health care provider may consider the alternative of just fulfilling any and all health data requests. However, while freely sharing data might reduce the complexity associated with information blocking, that action would not be consistent with a health care provider's existing HIPAA obligations.

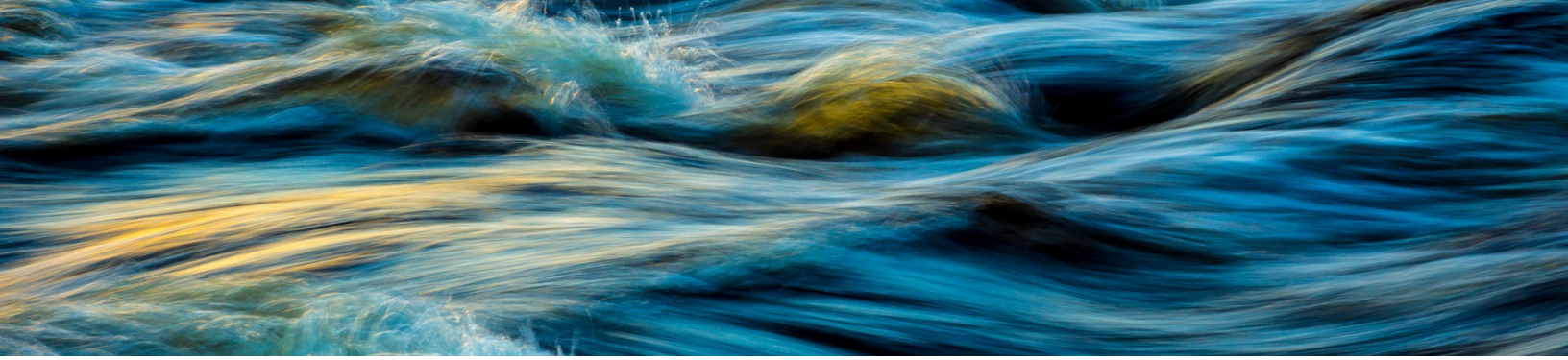
The penalty for information blocking for health care providers remains the "appropriate disincentives" referenced by the 21st Century Cures Act. The ONC final rule does not further detail these disincentives, suggesting that there may be additional rulemaking or clarification via other regulations. While the disincentives are not yet defined, it is in every health care provider's best interest to develop policies and procedures that fully comply with the information blocking requirements to avoid penalties for non-compliance.

[5] ONC has created an online portal to submit reports of information blocking; **https://www.healthit.gov/curesrule/final-rule-policy/information-blocking/report**



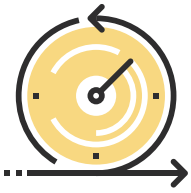
CMS's "Interoperability and Patient Access" Final Rule

Complementing the ONC rule, CMS also finalized requirements that generally apply to Medicare Advantage (MA) plans, Medicaid, and Children's Health Insurance Program (CHIP) managed care organization, state Medicaid and CHIP fee-for-service (FFS) entities, and Qualified Health Plans (QHPs) participating in the federally facilitated exchanges. These requirements are intended to support interoperability by encouraging use of APIs and increased digital data exchange. The CMS rule also includes two requirements for health care providers.



Electronic Notification Requirements

To help improve patient transitions between provider settings, CMS is revising the Medicare and Medicaid conditions of participation to require participating hospitals to send electronic notifications to another health care facility/provider when a patient is admitted, discharged or transferred (ADT). This requirement is only applicable to hospitals with an EHR system with the technical capacity to generate information for electronic patient event notifications. In addition, CMS does not require a specific standard to format or deliver these notifications, just a minimum content of at least a patient name, treating practitioner name and sending institution name.



Timeline

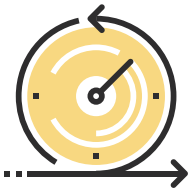
Health care providers will have twelve (12) months from rule publication to meet the ADT requirement. This represents an extension of 6 months, to allow flexibility for the COVID-19 response.

Implications for Health Care Providers

Health care providers should first confirm this requirement is applicable to them. If so, providers may consider whether they will be able and would like to utilize EHR capability, another vendor or build internal functionality.

Public Reporting of Providers

To discourage information blocking and possibly suggest health care providers that may be information blocking, CMS will publicly post information about providers who submit a "no" response to certain attestation statements related to the prevention of information blocking as part of the Medicare Quality Payment Program[6] and the FFS Promoting Interoperability Program. In addition to these attestations, CMS will also publicly report providers who fail to list their digital contact information to their entries in the National Plan and Provider Enumeration System (NPPES).



Timeline

CMS will publicly post this information in late 2020.

Implications for Health Care Providers

Providers already complete these attestation statements today, but now that these rules establish clear statutory and regulatory definitions for information blocking, providers may need to re-evaluate the processes in place to ensure compliance. Providers may need to evaluate what, if any, new functionalities in their certified EHR technologies they would utilize in order to be compliant. Health care providers should ensure coordinated conversations between HIM and departments traditionally responsible for these attestations.

[6]Please refer to CMS's fact sheet for the three attestation statements: **https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_InformationBlockingFact-Sheet20171106.pdf**

How to Address the Significant Implications for Health Care Providers

Make Robust Compliance Policies and Processes a Priority

The compliance responsibilities detailed in these final rules layer on top of existing regulations governing health care providers, such as requirements under HIPAA. These rules increase the considerations for a health care provider related to health data and health data exchange. In addition to simply understanding their new responsibilities, health care providers will also want to ensure they have robust tracking and reporting mechanisms to document health data requests and support any potential investigations. As mentioned earlier, information blocking exceptions have specific conditions that must be met and determination of information blocking will require interpretation. This means health care providers will benefit from proactively identifying any potential issues and documenting circumstances around requests.

Be Ready for Financial Disincentives That Begin November 2020

The information blocking prohibition in the 21st Century Cures Act has been in place since the bill was enacted into law in 2016. To date, however, OIG has not exercised its investigatory authority, instead waiting for the regulatory process to conclude. The final rule allows ONC to coordinate its review of a claim of information blocking with the OIG, defer to OIG to lead a review of a claim of information blocking, or allows ONC to rely on OIG findings to form the basis of a direct review action. Compliance with information blocking provisions goes into effect in November 2020, at which point health care providers will be responsible for any violations and associated appropriate disincentives.

Prepare for Digital Data Exchange At Scale

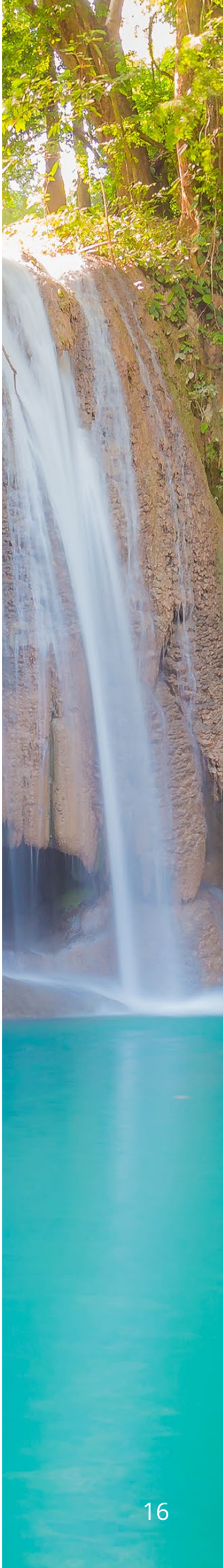
The healthcare industry has been historically slow to embrace change and innovation. However, these final rules and new requirements of payers and providers set a path for increased adoption of digital data exchange. Providers should prepare for increased volume and frequency of digital data exchange, which will still require some processes from today like validation of authorization for specific data elements. While exchange of clinical data may have historically occurred in person, in paper or electronically, hospital ROI processes and operations should prepare for a significant shift to digital exchange and digital data access management. A ROI process relevant for the future should have a technology platform that supports compliance, transparency and patient experience.

Employ a Cross-functional Approach to Enhance Operations

A primary impetus for the regulation is support for health record data exchange through APIs. While EHRs will be responsible for much of the technical work to make API exchange a reality, providers must adapt operations as well as define the governance for their electronic health information (e.g., determine criteria for API access permissions). This means that departments like HIM, Compliance and IT will need to work together to ensure there is a roadmap for digital health data exchange that meets the rule requirements as well as organizational needs. Further, health care providers may need to develop the infrastructure to assess the validity of API connections to protect themselves and their systems from breaches or other negative consequences.

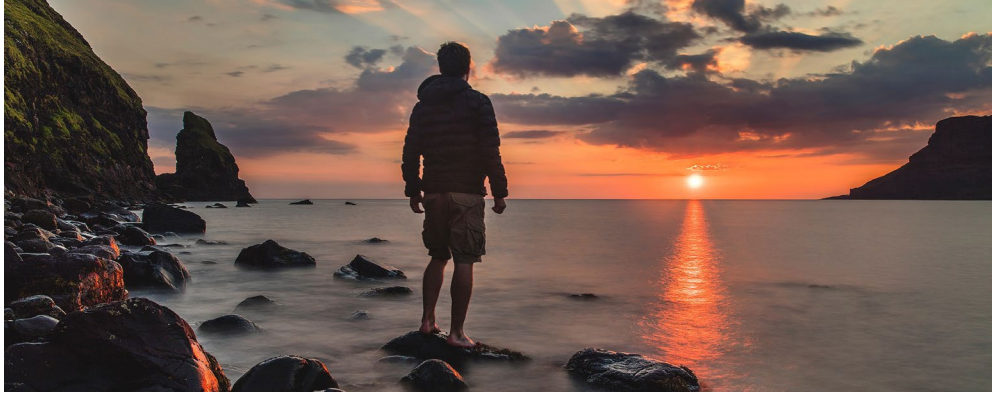
Educate Staff and Consumers

Given the operational and financial implications for health information management, health care providers should be prepared to educate their staff on any changes in how health record requests are logged, processed, and fulfilled. Consumers already are challenged in understanding their health data privacy rights. Considering an expected proliferation in health data connections, consumers may



be asked to direct their health data to even more non-covered entities, all without commensurate protections. While providers are not liable for consumers' choices, providers should prepare to respond to patient complaints and questions. We also recommend investing in proactive education, so patients are better prepared to make informed decisions about their health data rights.

These new rules from ONC and CMS mark the beginning of industry wide changes to further encourage digital data access and interoperability between digital systems. The sooner health care providers understand the direction of these changes and develop their own path towards that "north star," the better providers will be able to find the right partners to design processes and tools that best meet their needs and prepare their staff and patients for change. Leading providers will lean into these changes in ways that can supplement their goals around patient satisfaction and administrative efficiency. Achieving interoperability will be a journey and providers will be well served to prepare the right tools and find the right navigators.



Ciox Health, the nation's premier clinical data exchange and leading health technology company, is improving patient health by transforming clinical data into actionable insights. Combined with an unmatched network offering ubiquitous and secure access to healthcare data, Ciox's expertise, relationships, technology and scale make a difference for healthcare stakeholders and empower greater health for patients. Through its technology platform, which includes solutions for data acquisition, release of information, coding, data abstraction, and analytics, Ciox helps clients securely and consistently solve the last mile challenges in clinical interoperability. Ciox is proud to be ranked #1 in customer satisfaction for Interoperability Solutions by Black Book in 2020. Learn more about Ciox's technology and solutions by visiting **www.cioxhealth.com** or **Twitter** and **LinkedIn**.

cioxhealth.com/interoperability

interoperability@cioxhealth.com