ALSTON & BIRD

WWW.ALSTON.COM

Health Care / Privacy & Data Security ADVISORY ■

MAY 8, 2020

Expansive Interoperability and Data-Sharing Requirements Require Attention Despite Delays in Enforcement

by Elinor Hiller, Jane Lucas, Kate Hanniford, Sean Sullivan, Brian Lee, and Kathleen Benway

On April 21, 2020, the U.S. Department of Health and Human Services (HHS) announced that the HHS Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS) will exercise *enforcement discretion* for certain requirements in the final "interoperability" rules released in early March and published in the *Federal Register* on May 1, 2020. This announcement coincided with the release of an HHS Office of Inspector General (OIG) proposed rule related to enforcement of the prohibition of information blocking. Of note, the OIG proposes not to enforce information blocking penalties until 60 days after the release of the final rule. Comments to the OIG proposed rule are due by June 23, 2020.

Background

On March 9, 2020, HHS released the text of two final rules intended to expand patients' access to their health information. ONC finalized its 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program rule (the ONC Cures Act Final Rule), and CMS finalized its Interoperability and Patient Access rule (the CMS Final Rule) (collectively, the Interoperability Rules). New requirements will apply to health care providers, certain public and private payers, and states. The Interoperability Rules also establish standards and requirements for application programming interfaces (APIs) to support patient access and control of electronic health information (EHI).

The effects of these rules will be significant for providers and payers. The Interoperability Rules will lead to greater access to health information for patients (at no cost if accessed electronically) but will also create new data security and privacy considerations that regulated entities should heed as they stand up new systems and practices to comply. Combined, these final rules require health information-sharing between patients and other health-care-related parties through mandates effective as early as January 1, 2021.

Effective Dates and Enforcement Discretion

In light of the challenges the health care industry faces with the coronavirus (COVID-19), CMS and ONC will exercise enforcement discretion for various provisions of the Interoperability Rules. While compliance dates in the published Interoperability Rules remain the same as those in the initially released versions, CMS and ONC will not enforce certain requirements until later in 2021.

CMS stated that it will delay enforcement of certain requirement for **six months**. ONC stated that it will exercise enforcement discretion for all new requirements by extending the compliance dates and timeframes for **three months**.

Overview of effective dates and enforcement dates:

- **Patient Access API:** Effective 1/1/2021; enforcement discretion until 7/1/2021
- **Provider Directory API:** Effective 1/1/2021; enforcement discretion until 7/1/2021
- **Patient Access API for QHP Issuers:** Effective 1/1/2021; enforcement discretion until 7/1/2021
- **Hospital Conditions of Participation:** Effective 12 months after publication (5/1/2021)
- **ONC requirements:** Effective dates vary; enforcement discretion 6 months. Refer to table here.

Key CMS Final Rule Requirements

Requirements for plans

Patient Access API

Based on enforcement discretion offered, **by July 1, 2021**, CMS-regulated health plans are required to implement and maintain a "patient access API" that will allow data sharing with both enrollees and their third-party applications. This applies to Medicare Advantage (MA) organizations, Medicaid and Children's Health Insurance Program (CHIP) fee-for-service (FFS) programs, Medicaid and CHIP managed care plans/entities, and qualified health plan issuers on the federally facilitated exchanges (FFEs). The patient access API must meet the ONC Cures Act Final Rule technical standards (Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) Release 4.0.1 (HL7 FHIR)) as well as the content and vocabulary standards.

Through this API, payers must make available, and permit third-party apps to retrieve with the approval and at the direction of the patient:

- Adjudicated claims, including provider remittances and enrollee cost-sharing.
- Encounters with capitated providers.
- Clinical data, including laboratory results when they are maintained by the applicable payers.

The data must be made available within one business day after a claim is adjudicated or encounter data are received. When this requirement is enforced, applicable payers must maintain and be able to provide all specified data with a date of service on or after January 1, 2016.

Provider Directory API

Applicable payers are further required to make provider networks publicly available through a standards-based Provider Directory API, which will have to conform with the technical standards included in the ONC Cures Act Final Rule. **Provider Directory APIs must be fully implemented by July 1, 2021 due to the enforcement discretion**.

The Provider Directory API must be accessible through a public-facing digital endpoint on the payer's website. User authentication and authorization protocols are not required for this information because it will be publicly available to reach both current and prospective enrollees.

At a minimum, the Provider Directory API must include provider names, addresses, phone numbers, and specialties. MA organizations offering MA prescription drug plans also must include pharmacy directory data, including the pharmacy name, address, phone number, number of pharmacies in the network, and mix. Information must be updated within 30 calendar days of a payer receiving new or updated provider directory information.

Payer-to-Payer Data Exchange

Applicable CMS-regulated payers are required to exchange certain data elements finalized in the ONC Cures Act Final Rule, such as patient clinical data from the U.S. Core Data for Interoperability version 1 data set, upon a current or former enrollee's request. Payers are only required to share data received from another payer under this requirement in the electronic form and format that they were received.

The payer-to-payer data exchange must be fully implemented by January 1, 2022 and include data looking back up to five years. Note that enforcement discretion has not been offered on this deadline. This requirement applies to specified data that payers maintain with a date of service on or after January 1, 2016, to be provided to any other payer identified by a current or former enrollee.

Dually Eligible Enrollee Data Exchange

States are required to implement daily data exchange by April 1, 2022. This will increase the frequency—from monthly to daily—of federal and state data exchanges for individuals dually eligible for Medicare and Medicaid. This includes both sending data to and receiving responses from CMS daily.

Trusted Exchange Framework and Common Agreement

CMS did **not** finalize its proposal to require CMS-regulated payers to participate in a trusted exchange network.

Requirements for providers

Physicians and Clinicians

As part of its final rule, CMS will include on Physician Compare an indicator for eligible clinicians and groups that submit a negative response to the three prevention of information blocking statements for the Merit-based Incentive Payment System. This information will be posted on either the profile pages or in the downloadable database, beginning with the 2019 performance period data available for public reporting starting in late 2020. CMS also will publicly report the names and National Provider Identifiers for those providers that do not list or update their digital contact information (e.g., secure digital endpoints like a direct address or FHIR API endpoint) in the National Plan and Provider Enumeration System. This will begin the second half of 2020.

CMS also will include information on a publicly available CMS website indicating that an eligible hospital or critical access hospital attesting under the Medicare FFS Promoting Interoperability Program had a negative response to any of the three prevention of information blocking attestations. CMS will post this information beginning with the electronic health record reporting period in 2019, expected to be posted in late 2020.

Hospitals

CMS also modified the conditions of participation for hospitals, psychiatric hospitals, and critical access hospitals that utilize an electronic medical records system or other electronic administrative system (that conforms with the ONC Cures Act Final Rule requirements) requiring each hospital to demonstrate that:

- Its system's notification capacity is fully operational and in accordance with all state and federal requirements for the exchange of patient health information.
- Its system sends notifications that include certain patient health information (e.g., patient's name, treating practitioner name, and sending institution name).
- Its system sends notifications directly (or through an intermediary facilitating health information exchange) at the time of a patient's registration in and discharge/transfer from the emergency department or admission for inpatient services to all applicable:
  - Post-acute care providers and suppliers.
  - Primary care practitioners and groups and other practitioners and groups identified by the patient as primarily responsible for care that need to receive notification of the patient's status for treatment, care coordination, or quality improvement purposes.

These requirements will apply 12 months after publication of the CMS Final Rule. **This is a six-month delay of applicability, meaning these requirements will be effective starting May 1, 2021**.

Key ONC Cures Act Final Rule Requirements

The ONC rule includes significant new requirements for providers, health IT developers, and other entities engaged in the exchange of EHI, including plans.

Information Blocking

ONC's rule finalizes definitions implementing the 21st Century Cures Act prohibition against "information blocking." In general, information blocking refers to a practice by a health care provider, health IT developer, health information exchange, or health information network (referred to as "actors") that is "likely to interfere with access, exchange, or use of EHI."

In this final rule, ONC combined the definitions of health information exchange and health information network to create one broad definition ("actor") including an individual or entity "that determines, controls, or has the discretion to 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" among more than two unaffiliated individuals or entities enabled to exchange with each other for a treatment, payment, or health care operations purpose. This could include health plans engaged in this activity.

ONC revised its proposed definition of EHI to mean electronic protected health information as defined for HIPAA purposes, meaning actors will not have to separate electronic protected health information from EHI to comply with the HIPAA Rules and information blocking provisions. Note, however, that the definition excludes psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

ONC originally proposed seven specific allowed practices that would not be considered information blocking. ONC finalized eight exceptions that fall under the following policy considerations: (1) exceptions are limited to certain activities important to the successful functioning of the health care system; (2) each exception is intended to address a significant risk for regulated individuals and entities that would prevent reasonable and necessary activities; and (3) each exception is intended to be tailored such that it is limited to the reasonable and necessary activities it is designed to exempt.

The following eight exceptions available to actors involve requests to access, use, or exchange EHI:

1. ***Preventing Harm Exception*** – ONC finalized its proposal that actors may engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.

2. ***Privacy Exception (modified)*** – It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI to protect an individual's privacy, provided certain conditions are met. ONC modified this exception to more clearly place the obligation on the party requesting the EHI and the individual to attempt to satisfy the precondition by providing a consent or authorization.

3. ***Security Exception*** – Actors may interfere with the access, exchange, or use of EHI to protect the security of EHI, provided certain conditions are met.

4. ***Infeasibility Exception (modified)*** – It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met. ONC restructured this exception to include two discreet conditions related to uncontrollable events and an inability to "unambiguously segment" the requested EHI. ONC also removed the "reasonable alternative" requirement from this exception and incorporated it into the content and manner exception.

5. ***Health IT Performance Exception*** – Actors may take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.

6. ***Content and Manner Exception (new)*** – ONC added this exception to address comments about the required content and manner of a response to a request to access, exchange, or use EHI. Under this exception, limiting the content of the response, or the manner in which it fulfills a request to access, use, or exchange EHI (if certain conditions are met), would not be considered information blocking.

7. ***Fees Exception (modified)* –** ONC explicitly permits actors to charge fees, including those that result in a reasonable profit margin, for accessing, exchanging, or using EHI. ONC also clarified how this exception works with the licensing exception and the content and manner exception.

8. ***Licensing Exception (modified)* –** ONC clarified that an actor may condition access to and use of its interoperability elements for accessing EHI to acceptance of a license agreement, **if** its licensing program is applied in a nondiscriminatory manner and meets certain additional conditions.

ONC also released a timeline of key regulatory dates. Of note, ONC did not originally propose any delays in the implementation of the information blocking provisions. ONC finalized that **actors will have to comply with the information blocking rules six months after publication**. Further, ONC and the OIG are coordinating timing on the compliance date and start of enforcement. **Enforcement and civil monetary penalties will not begin until they are established by future OIG notice and comment rulemaking**.

ONC Health IT Certification Program

ONC finalized several additional requirements, including:

- **EHI Export Certification** – A certified Health IT Module must electronically export all EHI that can be stored at the time of certification by the product that the Health IT Module is a part of. Certified health IT developers must provide such capabilities to their customers within 36 months of the Final Rule's publication.

- **FHIR Standard for API Certification** – ONC adopted the HL7 FHIR standard as a foundational standard.

- **Communications Condition and Maintenance of Certification** – ONC established new provisions so that providers using certified health IT can communicate about usability, user experience, interoperability, and security. ONC clarified that screenshots and videos are forms of protected visual communications under this certification. ONC finalized that developers may, under permitted prohibitions and restrictions, restrict communications involving intellectual property so long as the prohibition or restriction is not broader than necessary and is consistent with other requirements. Further, developers may limit the sharing of screenshots and videos in certain circumstances.

Implications for Patients

Together, these final Interoperability Rules are intended to support and increase patients' control over their health care and medical records through the use of smartphones and software applications. As part of this, there is an expectation that these new interoperability requirements will provide information that will assist patients in making decisions about their care. Notably, the inclusion of cost-sharing information in the patient access API as well as the payer-to-payer exchange at the direction of the patient could provide greater opportunities for patients to track and monitor their health care utilization. As finalized, the ONC Cures Act Final Rule relies on the OAuth 2.0 protocol for authorization—a secure protocol used on travel and banking software applications—to ensure patient security. In addition, patients cannot be charged a fee to electronically access, exchange, or use their EHI.

Because patients will have the opportunity to push their data to third-party apps, there may be data security and privacy issues that providers, plans, and other actors should consider.

Key Considerations for Data Security and Privacy

Combined, the Interoperability Rules will have major implications across the health care system. In addition to having to stand up new mechanisms for data sharing and processing data requests, payers, providers, and other actors will need to consider data privacy and security implications as they design, develop, promote, and maintain these interoperability elements. The implementation of the Interoperability Rules may also raise broad security and privacy risk management considerations related to third-party access to patient data, such as authentication, patient education, liability, and privacy by design.

Privacy

HIPAA covered entities and their business associates will continue to be responsible for compliance with the HIPAA Security Rule, Privacy Rule, and Breach Notification Rule, which have not been altered or amended by these new final rules. However, once protected health information (PHI) from a patient's medical record is transmitted by an actor—at the patient's request—to a third-party vendor or third-party smartphone app, for instance, that data is no longer considered PHI to HIPAA, and the applicable covered entity (or business associate) that released the information no longer has any obligations under HIPAA for that third party's access to or use of that data. Note, though, that the covered entity (or business associate acting on the covered entity's behalf) is still responsible for implementing reasonable safeguards for the transit of PHI to a third party, even when pursuant to a patient's request, and that a covered entity may deny third-party

developers access to their API if that third party's application would present an unacceptable level of risk to the security of the PHI based on objective and verifiable criteria.

Additionally, HIPAA has always permitted covered entities to charge a "reasonable, cost-based fee" for providing copies of an individual's PHI. However, in requiring that patients have the ability to access their health information electronically *at no cost*, there were some concerns among vendors in the "release of information" (ROI) industry (which assists providers in responding to records requests, often by attorneys in personal injury cases) that the information blocking provisions of the ONC proposed rule could prevent them from charging for their services or otherwise put an end to their industry. But the final rule specifically identifies ROI services, and states that if it "meets all necessary conditions of the finalized exception [for charging fees], the actor *could* recover such categories of cost under the exception." The information blocking provisions appear to allow for ROI vendors to continue to charge covered entities and those requesting records for the production of patient medical information and to include "a reasonable profit margin."

Data security / cybersecurity

Although the ONC Cures Act Final Rule contains multiple provisions that may implicate cybersecurity considerations, two key sections in the rule pertain to communications of cybersecurity vulnerabilities and incidents as well as the potential to limit information-sharing based on security considerations. To the extent that the increased information-sharing pursuant to the final rule may potentially increase the overall risk for cybersecurity incidents, these two aspects of the rule together preserve the ability to communicate cybersecurity vulnerabilities and incidents but also create a limited exception to restrict information-sharing with health IT based on security considerations.

<u>Communications of cybersecurity vulnerabilities and incidents (Sections 170.403(a)(1)(iii) and (a)(2)(i))</u>

The ONC Cures Act Final Rule makes clear that health IT developers cannot restrict communications of cybersecurity vulnerabilities or incidents. In addition, while the rule does not explicitly impose separate requirements for developers on the sharing of cybersecurity vulnerabilities with health care providers, ONC explicitly reiterates that HHS "expect[s] developers with Health IT Modules certified under the Program to share information about cybersecurity vulnerabilities with health care providers and other affected users as soon as feasible," for the stated purpose of assisting affected users' mitigation of the potential impact of any such vulnerabilities "on the security of EHI and other [personally identifiable information] in the users' systems." Although users are not required to notify the developer of cybersecurity vulnerabilities or issues they may discover, they are "strongly encourage[d]" to do so.

<u>Security Exception to Information Blocking (Section 171.203)</u>

The ONC Cures Act Final Rule includes a security exception to the information blocking definition. This exception permits actors to engage in "security-motivated" practices that would otherwise be considered unlawful information blocking provided that such practices "are reasonable and necessary to promote the security of EHI." To be eligible for this exception, the practice must be:

- Directly related to the safeguarding of confidentiality, integrity, and availability of EHI (i.e., the practice should be actually necessary and directly related to the specific security risk being addressed).
- "Tailored to the specific security risk being addressed."
- Applied consistently and without discrimination.

In addition, actors must meet criteria depending on whether the practice implements an organizational security policy. For practices that implement an organizational security policy, the policy must be documented in writing, supported by a risk assessment, and aligned with a recognized standard or best practices guidance (e.g., ISO, NIST). If the practice does not implement an organizational security policy, the actor must make a determination in each case that the practice is necessary to mitigate the specific security risk to EHI and that there are no reasonable or appropriate alternatives.

Whether a "security-motivated practice" can meet this exception will be determined on "a case-by-case basis using a fact-based analysis," consistent with the HIPAA Security Rule's requirement for covered entities and business associates to develop and implement appropriate administrative, physical, and technical safeguards. However, "the fact that a practice complies with the HIPAA Security Rule would not establish that it meets the conditions of the exception to the information blocking provision."

The security exception may be especially relevant when read in tandem with the ONC Cures Act Final Rule's privacy and security transparency attestations, which are intended to provide transparency by identifying whether certified health IT supports encrypting authentication credentials and multifactor authentication. To the extent that an attestation indicates that the health IT does not support encryption of authentication credentials or multifactor authentication, these could be grounds for additional scrutiny by an actor under the security exception to information-sharing.

However, the ONC Cures Act Final Rule adopts the OAuth 2.0 standard for Health IT Modules' implementation of an API to minimize security risks to patients, despite acknowledging that this standard is susceptible to cross-site request forgery vulnerabilities. To mitigate this risk, the rule encourages "implementers to adhere to industry best practices" and points to the HL7 Implementer's Safety Check List to guide implementation of APIs. Although the rule acknowledges the tension between data security and authentication procedures on one hand, and the interests of health IT, patients, providers on the other, it also cautions certified Health IT Modules against requiring patients to reauthorize or reauthenticate with such frequency that it would be considered information blocking.

FTC considerations

Following issuance of the final rules, the Federal Trade Commission (FTC) staff issued a letter to ONC expressing appreciation for including changes to the ONC Cures Act Final Rule that the FTC had suggested to ensure that the rule did not "inadvertently distort competition or impede innovation." The FTC noted that several changes reflected in the final rule "will likely further [the agencies'] joint goals of fostering procompetitive innovation in health IT while protecting patient privacy." The FTC specifically noted the following improvements:

- A streamlined definition of EHI will apply more narrowly to information of concern to the Cures Act.
- The addition of a content and manner exception to the prohibition on information blocking will facilitate near-term compliance with the rule's requirements for EHI.
- Clarification and streamlining of "exchange, access, and use" concepts.

The FTC also noted its appreciation of ONC's clarification that the final rule does not alter the FTC's role in protecting the privacy and security of consumer's personal information. The FTC gave examples of where it has or could take enforcement action to prevent unfair or deceptive practices related to health information, including against a health IT app developer whose privacy promises departed from its practices. It also noted that it could challenge a particular use or disclosure of health information as "unfair" if it caused or was likely to cause substantial consumer injury not reasonably avoidable by the consumer and not outweighed by countervailing benefits to the consumer and competition.

Alston & Bird has formed a multidisciplinary task force to advise clients on the business and legal implications of the coronavirus (COVID-19). You can view all our work on the coronavirus across industries and subscribe to our future webinars and advisories.

You can subscribe to future ***Health Care*** and ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please visit our **Health Care** and **Privacy & Data Security** groups or contact any of the following:

Elinor A. Hiller
202.239.3766
elinor.hiller@alston.com

Jane B. Lucas
202.239.3229
jane.lucas@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

Sean Sullivan
404.881.4254
sean.sullivan@alston.com

Brian Lee
202.239.3818
brian.lee@alston.com

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333