Health Industry Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Interoperability and Information Blocking: What Providers, Payers and IT Developers Need to Know about New Enforcement Timelines

November 4, 2020

Key Points

- On May 1, 2020, the ONC Interoperability, Information Blocking and Health IT Certification Program Final Rule and the CMS Interoperability and Patient Access Final Rule were published in the Federal Register, marking the start of the implementation timetables for these major regulations.
- In light of the COVID-19 pandemic, on October 29, 2020, ONC released an interim final rule further pushing out compliance dates for the new information blocking regulations, certain health IT certification criteria, and the Conditions and Maintenance of Certification Requirements under the Health IT Certification Program.
- Enforcement timelines remain unclear, as the HHS Office of Inspector General has yet to issue a final rule on how it will enforce the information blocking provisions against health IT vendors, health information exchanges and health information networks, and HHS has yet to make any proposal regarding enforcement against providers.

Just days prior to President Trump's declaration of a national emergency on March 13, 2020, the U.S. Department of Health and Human Services (HHS) rolled out two significant final regulations aimed at bolstering the accessibility and exchange of electronic health information (EHI). These final regulations were published in the Federal Register on May 1, 2020, marking the start of the implementation timetables. While the Administration remains committed to this regulatory regime, various delays have been announced in light of the pandemic crisis.

On April 21, HHS announced it would delay enforcement of these final rules, which otherwise were set to become effective June 30, 2020. The reason for the delayed enforcement, according to HHS, was "to allow compliance flexibilities . . . in response to the coronavirus disease (COVID-19) public health emergency." On October 29, 2020, HHS issued an interim final rule further extending certain compliance dates and timeframes due to the ongoing COVID-19 pandemic (the "Interim Final Rule").

Contact Information

If you have any questions about this Alert, please contact:

Kelly M. Cleary
Partner
kcleary@akingump.com
Washington, D.C.
+1 202.887.4020

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Mallory A. Jones
Associate
jonesm@akingump.com
Washington, D.C.
+1 202.887.4259

For the new information blocking penalties, the enforcement timetable will depend on when HHS finalizes regulations implementing its new enforcement authorities. On April 21, HHS took an important step toward implementing its new civil monetary penalty (CMP) authority. The HHS Office of Inspector General (OIG), charged by Congress with investigating the information blocking practices of providers, IT developers, health information exchanges (HIEs) and health information networks (HINs), issued a proposed rule that would, among other things, allow the OIG to impose CMPs—up to $1 million per violation—on those actors found to have knowingly interfered with the access, use or exchange of EHI.

This client alert highlights important information for providers, payers and health IT developers regarding the new enforcement timelines.

Overview of Recent Regulatory Activity

The ONC Interoperability, Information Blocking and Health IT Certification Program Final Rule ("ONC Final Rule")

On March 9, 2020, the Office of the National Coordinator for Health Information Technology (ONC), which is charged with supporting the adoption of health information technology, released long-awaited regulations implementing certain provisions of the 21st Century Cures Act (the "Cures Act") meant to advance interoperability and support the access, exchange and use of EHI, including significant changes to ONC's Health IT Certification Program.[1]

One key component of the Final Rule is the implementation of Section 4004 of the Cures Act, which created new federal penalties to deter the practice of information blocking. Broadly speaking, information blocking is any practice that may interfere with the use, access or exchange of EHI and that is not "reasonable and necessary." The Final Rule establishes key definitions around the individuals and entities that are "covered actors" subject to penalties for information blocking. It also finalizes exceptions to the definition for activities that are "reasonable and necessary," including a "content and manner" exception that will allow covered actors to restrict content to a more limited set of EHI. Compliance with these regulations was initially required by November 2, 2020. In the Interim Final Rule, ONC pushes back the compliance date until April 5, 2021.[2]

Importantly, the Final Rule also gives covered actors an additional 18 months after the initial compliance date during which they will only be required to provide data elements represented in the U.S. Core Data for Interoperability (USCDI) in response to a request to access, exchange or use EHI, rather than the full scope of EHI. To maintain this transition period, in the Interim Final Rule, ONC updates the date by which actors must provide all EHI in response to a request to October 6, 2022. The scope of data included in the USCDI is significantly more limited than the full definition of EHI, which includes all individually identifiable health information transmitted or maintained in electronic form that would be included in a designated record set under HIPAA[3], regardless of whether the records are used or maintained by or for a covered entity (with certain exceptions). The USCDI, on the other hand, is a defined set of data elements within certain overarching categories, including clinical notes, patient demographics and vital signs.[4]

The Final Rule also establishes new Conditions and Maintenance of Certification requirements for health information technology ("health IT") developers under the ONC

Health IT Certification Program, and standards for the voluntary certification of health IT for use by pediatric health care providers.[5] Among other conditions, the ONC Final Rule requires as Conditions of Certification that a health IT developer not take any action that constitutes "information blocking" and that a health IT developer provide assurances to the agency that it will not take any such action (unless for certain legitimate purposes) or any other action that may inhibit the appropriate exchange, access and use of EHI.

ONC also adds new API Conditions of Certification that address the practices developers of certified health IT should engage in, such as minimizing the "special effort" necessary to access, exchange and use EHI via certified API technology. Compliance with these Conditions of Certification was initially required by November 2, 2020. However, in the Interim Final Rule, the agency pushes back the compliance date to April 5, 2021.

CMS Interoperability and Patient Access Final Rule ("CMS Final Rule")

Centers for Medicare & Medicaid Services (CMS) issued a final regulation in tandem with the ONC Final Rule geared toward interoperability and patient access to health information. The CMS Final Rule[6] creates new data-sharing standards for payers participating in Medicare Advantage (MA), Medicaid, CHIP and the Federally-facilitated Exchanges (FFEs). Two of the new requirements to implement and maintain standards-based APIs (for claims and encounter information and provider directory information) are due to take effect on January 1, 2021, but CMS said it will delay enforcement for six months, until July 1, 2021.

CMS has also modified its Medicare Conditions of Participation (CoPs) to require hospitals, including psychiatric hospitals and critical access hospitals, to send electronic patient event notifications of a patient's admission, discharge and/or transfer to another healthcare facility or to another community provider or practitioner. According to CMS, these measures will improve care coordination by allowing a receiving provider, facility or practitioner to reach out to the patient and deliver appropriate follow-up care in a timely manner. These CoPs will be applicable May 1, 2021, or 12 months after publication of the Final Rule.

OIG Civil Monetary Penalty Rule

On April 21, OIG issued a proposed rule implementing new CMP authorities, including the Cures Act CMP authority at Section 4004.[7] Section 4004 of the Cures Act added Section 3022 to the Public Health Service Act (PHSA), which, among other provisions, provides OIG the authority to investigate claims of information blocking and authorizes the Secretary to impose CMPs against a covered actor that OIG determines committed information blocking.[8] In the proposed rule, OIG proposes to implement Section 3022(b)(2)(C) by adding the information blocking CMP authority to the existing regulatory framework for the imposition and appeal of CMPs, assessments and exclusions.[9]

The proposed rule also explains OIG's anticipated approach to enforcement and coordination within HHS to implement the information blocking authorities. OIG explains that it will likely focus its enforcement efforts on conduct that: (i) resulted in, is causing or had the potential to cause patient harm; (ii) significantly impacted a provider's ability to care for patients; (iii) was of long duration; (iv) caused financial loss to federal health care programs, or other government or private entities; or (v) was

performed with actual knowledge. OIG further explains that it will "closely coordinate" with ONC given its separate authority under the PHSA to regulate information blocking and its expertise on the information blocking regulations. Furthermore, OIG will be referring information blocking claims to OCR if consultation regarding HIPAA regulations would "resolve" an information blocking claim.

What Providers Need to Know

Health care providers are "covered actors" under the information blocking rules, but HHS has yet to propose a specific enforcement mechanism.

A health care provider is a "covered actor" under the information blocking rules and may be subject to sanction if found to have knowingly engaged in any practice that "is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." Notably, HHS elected to use the broad definition of "health care provider" in the PHSA, which includes facilities like hospitals, ambulatory surgical centers, labs, pharmacies and nursing facilities, as well as individual practitioners like physicians and pharmacists.[10]

OIG is charged with investigating allegations of information blocking and determining whether a violation has occurred. However, unlike other covered actors subject to the information blocking rules, health care providers are not subject to the $1 million-per-violation CMPs under Section 4004 of the Cures Act. Rather, Congress directed OIG to refer provider violations to "the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking."[11] HHS has yet to identify the agency or agencies that will handle information blocking referrals, and also has yet to identify the "disincentive" that will apply to providers that engage in information blocking.

While a provider-specific information blocking enforcement policy is being developed, health care providers may still be subject to other adverse action if practices violate HIPAA right of access or Medicare payment rules.

While the provider-specific information blocking enforcement mechanism will take time to develop and implement through rulemaking, other authorities already in existence could serve as a basis for the sanction of health care providers.

For covered actors that are also covered entities under the Health Insurance Portability and Accountability Act of 1996 and Health Information Technology for Economic and Clinical Health Act of 2009 (together with their implementing regulations, HIPAA), some conduct that constitutes information blocking could potentially be punishable as a violation of a patient's right of access under existing authority. The HHS Office for Civil Rights (OCR) investigates alleged HIPAA violations, and has the authority to impose CMPs of up to almost $1.8 million per violation.[12] Many OCR investigations end in a settlement agreement accompanied by a corrective action plan—the highest settlement payment to date is $16 million.[13]

For covered actors that participate in the Medicare Quality Payment Program or Medicare and Medicaid Promoting Interoperability Program, engaging in practices that are considered information blocking could affect performance scores and payment adjustments under those programs. Further, CMS has said that it would begin publicly reporting providers that may be failing to comply with certain information sharing expectations in "late 2020." The agency explained that it will name providers who do

not list or update their digital contact information in the National Plan and Provider Enumeration System (NPPES). CMS will also report eligible clinicians, hospitals and critical access hospitals that may be information blocking based on how they attested to certain Promoting Interoperability Program requirements in data collected for the 2019 performance year.

Health care providers that meet the definitions of HINs or HIEs may be subject to CMPs, but not before OIG finalizes its proposals.

Notably, in the ONC Final Rule, ONC emphasized that the definitions of HIE and HIN are functional definitions, meaning that they will include any individual or entity that performs certain functional activities. In its proposed rule, OIG pointed out that some health care providers may meet the definition of an HIN or an HIE. In cases where a health care provider is acting in its capacity of one of these other "covered actors," the provider may be subject to CMPs under the Cures Act.[14] For example, if a large health care provider leads an effort to establish a network that facilitates the movement of EHI between itself and a group of smaller health care providers through health IT, the large health care provider could come within the definition of an HIN or HIE.[15]

For providers subject to the new Medicare Conditions of Participation, enforcement will be delayed 12 months (until May 1, 2021).

The CMS Final Rule requires, as a condition of participation in the Medicare program, that hospitals, including psychiatric hospitals and critical access hospitals, send electronic notification of a patient's admission, discharge or transfer to another health care facility, community provider or other practitioner. Failure to meet a condition of participation could ultimately result in the termination of a hospital's Medicare provider agreement. This requirement was originally set to take effect six months after the rule was published in the Federal Register. CMS has extended this implementation timeline to 12 months after the rule is published, or May 1, 2021.[16]

What Payers Need to Know

Payers are not specifically identified as "covered actors" under the information blocking rules, but could be subject to enforcement if functioning as an HIN or HIE.

Payers are not subject to the information blocking rules and penalties unless they meet the functional definition of one or more "covered actor"—i.e., a developer or offeror of HIT, an HIE or an HIN. As noted above, in its final rule, ONC explained that the definitions of HIE and HIN are functional definitions, meaning that they will include any individual or entity that performs certain functional activities. Payers should understand these definitions and determine whether they may be subject to the new information blocking rules and penalties.[17]

Payers offering plans in Medicare, Medicaid, CHIP and the Federally-facilitated exchanges must meet new data access and sharing requirements, but CMS has delayed enforcement of certain requirements until July 1, 2021.

Payers that participate in one or more federal health care programs will also need to understand the new CMS requirements for data access and exchange. The regulations finalized in the CMS Final Rule apply to Medicare Advantage (MA) organizations; Medicaid fee-for-service (FFS) programs and managed care plans; Children's Health Insurance Program (CHIP) FFS programs and managed care plans;

and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs), with certain exceptions (collectively, "covered payers").

The CMS Final Rule imposes the following requirements on covered payers:

- *Patient Access Application Programming Interface (API)*. Covered payers must implement and maintain a secure, standards-based API that affords patients easy access to their claims and encounter information, including cost and certain clinical information, through third-party applications of their choice. Under the CMS Final Rule, covered payers are required to implement this patient access API beginning January 1, 2021. QHP issuers on the FFEs are required to implement it for plan years beginning on or after January 1, 2021. However, CMS has announced that it will not enforce this requirement for any covered payer until July 1, 2021.[18]
- *Provider Directory API*. Covered payers[19] must make provider directory information publicly available via a standards-based API. Under the CMS Final Rule, payers are required to implement this provider directory API by January 1, 2021, but CMS will not enforce this requirement until July 1, 2021.[20]
- *Payer-to-Payer Data Exchange*. Covered payers must exchange certain patient clinical data with other payers at the patient's request. Covered payers are required to implement a process for this data exchange beginning January 1, 2022. QHP issuers on the FFEs are required to implement this process for plan years beginning on or after January 1, 2022.

Depending on payer type, failure to meet these requirements could affect a program or plan's participation in the Medicare, Medicaid or CHIP programs, or on the FFEs.

What Health IT Developers Need to Know

Health IT developers and other entities that offer certified health IT are "covered actors" under the information blocking rules, and will be subject to CMPs once the OIG's CMP rule is finalized and becomes effective.

Developers of health IT, entities offering certified health IT, HIEs, HINs, and, as noted above, health care providers are among the individuals and entities that Congress identified as "covered actors" subject to penalty for information blocking. Such entities are therefore subject to OIG investigation and (except for providers) CMPs for engaging in practices that the entities know or should know are likely to interfere with, prevent or materially discourage access, exchange or use of EHI.[21] Once OIG determines that an individual or entity has engaged in information blocking, the Cures Act mandates a penalty of up to $1 million per violation for covered actors other than health care providers.

In its proposed rule, the OIG stated that it would not begin enforcing the information blocking CMPs until the final rule is issued and the regulations become effective (likely 60 days from the date of publication of a final rule). Depending on how quickly the regulations become finalized, it is possible that OIG enforcement will begin before the end of this year. For IT developers and other covered actors that have heretofore not been subject to direct HHS regulation and enforcement, understanding compliance obligations and OIG enforcement priorities is critically important.

For developers of certified health IT, compliance with the new conditions of certification for information blocking and APIs are delayed until April 5, 2021.

Developers of certified health IT will need to comply with the new ONC standards for obtaining and maintaining certification. The regulations establishing these standards technically became effective on June 30, 2020, but ONC delayed the compliance date for many of the new requirements in the ONC Final Rule. In the Interim Final Rule, ONC again pushes back certain compliance dates until April 5, 2021.

Here are some of the key compliance and effective dates for the new certification conditions related to interoperability and information blocking for certified health IT.

[1] U.S. Dept. of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology (ONC), 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, Final Rule, 85 Fed. Reg. 25,642 (May 1, 2020), https://www.govinfo.gov/content/pkg/FR-2020-05-01/pdf/2020-07419.pdf [hereinafter "ONC Final Rule"].

[2] In the Interim Final Rule, ONC explains that it will refer to this date as the "applicability date," instead of the "compliance date." HHS ONC, Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency, Interim Final Rule with Comment Period, 85 Fed. Reg. 70,064 (Nov. 4, 2020), https://www.govinfo.gov/content/pkg/FR-2020-11-04/pdf/2020-24376.pdf.

[3] "HIPAA" refers to the regulations implementing the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009, codified at 45 C.F.R. Parts 160, 162 and 164.

[4] HHS, ONC, United States Core Data for Interoperability (USCDI), Version 1 (July 2020 Errata) at 4, https://www.healthit.gov/isa/sites/isa/files/2020-10/USCDI-Version-1-July-2020-Errata-Final_0.pdf.

[5] The 21st Century Cures Act directed ONC to develop Maintenance of Certification requirements, which require certified health IT vendors to demonstrate continued compliance with certain standards after initial certification.

[6] Centers for Medicare & Medicaid Services (CMS), Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-facilitated Exchanges, and Health Care Providers, Final Rule, 85 Fed. Reg. 25,510 (May 1, 2020), https://www.govinfo.gov/content/pkg/FR-2020-05-01/pdf/2020-05050.pdf [hereinafter "CMS Final Rule"].

[7] HHS, Office of Inspector General (OIG), Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Monetary Penalty Rules, Proposed Rule, 85 Fed. Reg. 22,979 (Apr. 24, 2020).

[8] 42 U.S.C. § 300jj-52.

[9] 42 C.F.R. Parts 1003 and 1005.

[10] 42 U.S.C. § 300jj(3).

[11] *Id*. § 300jj-52(b)(2)(B).

[12] 45 C.F.R. §§ 160.404, 102.3.

[13] HHS, ONC, Anthem pays OCR $16 Million in record HIPAA settlement following largest health data breach in history (Oct. 15, 2018), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html (last accessed Oct. 29, 2020).

[14] 85 Fed. Reg. at 22,981 (explaining that health care providers could be subject to civil monetary penalties if they meet the definition of one or more "covered actor").

[15] ONC Final Rule at 25,801.

[16] CMS Final Rule at 25,603.

[17] *See* ONC Final Rule at 25,802–03 (declining a request from commenters to exclude payers or other specific entities from the definition of HIE or HIN).

[18] CMS, CMS Interoperability and Patient Access Final Rule, https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index (last accessed Oct. 29, 2020).

[19] QHP issuers on the FFEs are already required to make provider directory information available in a specified, machine-readable format.

[20] *Id*.

[21] The intent requirement for providers is different, and liability requires a showing that the conduct was both unreasonable and that the provider knew that it was likely to interfere with, prevent or materially discourage access, exchange or use of EHI. 42 U.S.C. § 300jj-52(a)(1)(B)(ii).