Access to Health Information & Interoperability of Health Information Technology

Summary

On May 1, 2020, the Department of Health and Human Services (HHS), through the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC), issued final rules seeking to improve patient access to health data and to support the interoperability of Health Information Technology (Health IT). This Issue Brief outlines the key elements of these changes and their impact on health insurance providers.

Who should read this?

- Chief Information Officers
- Chief Medical Officers
- Chief Innovation Officers
- Privacy Officers
- Legal Counsels
- Provider Contracting
- Business Operations

What are the Key Implications for Health Insurance Providers?

- The final rules seek to establish patients as the owners of their health information with the right to direct its transmission by health insurance providers to third-party application (app) developers in a free and convenient way.
- The scope of data to be shared by health insurance providers is extensive, including provider payment amounts, patient cost-sharing, clinical data, formularies, and provider directory information.
- Standardized web-based technology must be employed in a 'pro-competitive' manner and enrollees must be proactively advised that they are not required to use only the health insurance provider's own preferred applications.
- Health insurance providers must educate enrollees on what to look out for in terms of the privacy and security of apps and may share whether the apps have attested to certain practices, but they may not deny a connection with any secure app developer elected by the patient.
- The implementation timeframe is short with the web-based technology and plan data sharing required to be in place by July 1, 2021. While the effective date is technically January 1, 2021, CMS instituted a 6-month period on enforcement discretion given the COVID-19 pandemic.
- While the CMS rule precludes health insurance providers from charging the apps, it acknowledges that the increased costs associated with maintaining the technology may be incorporated in bids.
- ONC finalized a vague definition of "actors" subject to "information blocking" penalties and chose not to exclude any particular types of organizations, leaving significant questions as to the breadth of organizations to which the potential million-dollar-per-instance penalties may apply.
- These interoperability rules interact with the Administration's many transparency rules applicable to both hospitals and health insurance providers seeking to increase the availability of health care services pricing information to consumers and apps that may serve them.
- We expect additional proposed rulemaking in the fall of 2020 extending the interoperability rules to additional use cases discussed but not finalized in these rules.

Interoperability means the secure exchange of electronic health information without special effort on the part of the user. It allows for complete access, exchange and use of all authorized information, and thus is not considered information blocking.

Why did CMS and ONC issue the proposed rules?

The final rules include policy changes designed to support the Administration's *MyHealthEData* initiative, which is intended to empower patients with access to their health information through whatever device or app they choose with the goal of fostering choice and competition in health care.

CMS launched Blue Button 2.0 in 2018 as part of the *MyHealthEData* initiative, which enabled enrollees in traditional Medicare to access their health care claims information electronically, through an app of their choosing. The CMS interoperability final rule continues to build on these efforts by requiring private health insurance providers who do business with the federal government to implement comparable access programs.

In tandem, the ONC final rule implements certain provisions of the 21st Century Cures Act. This final rule promotes complementary policies that ensure a patient's electronic health record information is accessible to that patient electronically through their doctor or hospital at no cost. It also adopts the data and technical standards for the web-based technology that health insurance providers must adhere to under the CMS policies.

Together, the final rules seek to make patient data more useful and transferable through open, secure, standardized, and machine-readable formats.

Application Program Interface (API) is code that allows two software programs to communicate with each other. The API defines the correct way for a developer to write a program that requests services from an operating system or other application. For example, consider how application (app) developers can make their services available on an iPhone. Apple provides sufficient information for a developer to create software that can interact and exchange information on an iPhone.

Fast Healthcare Interoperability Resources (FHIR, pronounced "fire") is an interoperability standard developed by Health Level 7 International (HL7) describing data formats and elements (known as "resources") and an application programming interface (API) for exchanging electronic health information.

The U.S. Core Data for Interoperability (USCDI) specifies a common set of data classes that are required for interoperable exchange. For example, this currently includes but is not limited to lab results, clinical notes, demographics, medications, etc.

What are the key provisions in the CMS final rule?

Applicable Health Insurance Providers

The final CMS policies apply to Medicare Advantage (MA) organizations, including MA Health Maintenance Organization (HMO), MA Point-of-Service (POS), and MA Preferred Provider Organization (PPO); Medicaid managed care plans, state Medicaid Fee-for-Service (FFS); CHIP managed care entities, and CHIP agencies that operate FFS systems, and qualified health plans (QHP) in the federally facilitated exchanges (FFE).This final rule does not apply to Medicare Cost Plans, stand-alone Prescription Drug Plans (PDP), or Program of All-Inclusive Care for the Elderly (PACE) organizations. Additionally, Stand-Alone Dental Plans (SADP) in the FFE as well as the Federally facilitated Small Business Health Options Program Exchanges (FF-SHOP) are excluded from these policies.

Key Deadlines

- **January 1, 2021, Enforceable July 1, 2021** – Deploy Patient Access API. As a result of the COVID-19 pandemic and to provide additional flexibility to payers, CMS instituted a 6-month enforcement discretion period for this provision.
- **January 1, 2021, Enforceable July 1, 2021** – Deploy Provider Directory API. As a result of the COVID-19 pandemic and to provide additional flexibility to payers, CMS instituted a 6-month enforcement discretion period for this provision.
- **January 1, 2022** – Deploy Payer-to-Payer Data Exchange. CMS did not provide for a period of enforcement discretion for this provision.

Patient Access API

Health insurance providers must deploy a Patient Access API to share claims and clinical information maintained by the payer for dates of service on or after January 1, 2016 with third-party apps at the patient's request.

Required Data Elements

CMS defines "maintained" as data the health insurance provider has access to, control over, and authority to make available through the API.

The minimum requirements for the Patient Access API are:

- Adjudicated claims;
- Encounters with capitated providers;
- Provider remittances;
- Enrollee cost-sharing;
- Clinical data;
- Formularies or preferred drug lists for all impacted payers (except QHP issuers on the FFEs)

For MA organizations that offer an MA-PD plan (not stand-alone Prescription Drug Plans), the additional provisions are required below:

- Data concerning adjudicated claims for covered Part D drugs, including remittances and enrollee cost-sharing, no later than 1 business day after a claim is adjudicated; and
- Formulary data that includes Part D drugs and any tiered formulary structure or utilization management procedure which pertains to those drugs.

Data must also be available in the Patient Access API no later than 1 business day after a claim is adjudicated or encounter data is received by the impacted payer.

Required Standards

The CMS rule relies on a combination of standards finalized in its rule and the ONC's rule:

- Claims— ASC X12N 837 as the relevant content and vocabulary standard for the claims information.
- Clinical— United States Core Data for Interoperability (USCDI) version 1 [July 2020 Errata] as the relevant content and vocabulary standard for the clinical information required. Attachment 1 summarizes the elements in the USCDI.
- Formulary— National Council for Prescription Drug Programs (NCPDP) Script Standard as the relevant technical, content and vocabulary standard.
- Technical— Foundational Health Level 7 (HL7®) and its complementary security and app registration protocols (OAuth 2.0 and OpenID Connect Core) as the technical standard for the exchange of the information.

OAuth 2.0 is the industry-standard protocol for authorization within web applications, desktop applications, mobile phones, and living room devices.

Open ID Connect 1.0 is a layer on top of the OAuth 2.0 protocol that verifies the identity of the end-user.

CMS references several HL7 Implementation Guides (IG) to further support sharing the needed data using the required standards:

- Claims and Encounter Data— CARIN Alliance Blue Button® Framework and Common Payer Consumer Data Set (CPCDS) IG.
- Clinical Data— Payer Data Exchange (PDex) IG or the US CORE IG.
- Plan Coverage and Formularies— DaVinci Payer Data Exchange US Drug Formulary IG.

Privacy and Patient Consent

Health insurance providers must include and emphasize the importance of understanding the privacy and security practices of any app to its enrollees. This information must be in "non-technical, consumer-friendly language" and include information on how to submit complaints to the Federal Trade Commission (FTC) and the Department of Health & Human Services (HHS). CMS provides consumer educational materials and recommendations in its Patient Privacy and Security Resources.

All obligations under state and federal law, including HIPAA, remain in place and are not diminished by this rule. Covered entities must protect the privacy and security of information, including but not limited to personal health information (PHI). CMS points to industry best practices, including the CARIN Alliance's Code of Conduct and the ONC Model Privacy Notice for provisions health insurance providers may choose to include in their attestation requests of app developers to disclose to patients. However, it is important to note that health insurance providers may not require any sort of certification or deny any connection request from an app at the direction of a patient unless it poses a threat to the security of their own systems.

Provider Directory APIs

Health insurance providers must also develop and deploy standardized web-based technology to allow third-party app developers to create tools for patients to search for providers, as well as providers to search for other providers, to better facilitate care coordination. The Provider Directory API does not require a patient to elect the sharing of data like the Patient Access API. It is intended to be publicly available to enable apps to build in provider directory data for consumers shopping for insurance rather than just those who have already purchased it. QHPs in the FFEs are not required to offer the API but must maintain machine-readable files per that program's requirements.

Required Data Elements

The Provider Directory API must include provider and pharmacy names, addresses, phone numbers, and specialties. For Medicare Part D (MA-PD) plans, the number of pharmacies and the type of pharmacy must also be included.

All directory information must be made available through APIs within 30 calendar days of a payer receiving the directory information or an update to that information.

Required Standard

The CMS rule requires the use of the following standard:

- Technical— Foundational Health Level 7 (HL7®).

CMS references the following HL7 IG to further support sharing the needed data using the required standards:

- Provider Directory— DaVinci PDEX Plan Net IG.

Payer to Payer Exchange

The final rule requires the exchange of certain patient clinical data (specifically the USCDI version 1 data set) between payers at a patient's request. This is intended to allow patients to take their information with them as they move from payer to payer over time. This requirement is effective January 1, 2022, for data maintained with a date of service on or after January 1, 2016, and must cover the duration of enrollment as well as 5 years after coverage ends. For QHP issuers on the FFEs, this requirement applies to plan years beginning on or after January 1, 2022. CMS did not dictate a particular technical standard for the exchange of this information, but rather left it to the discretion of the health insurance providers.

What are the key provisions in the ONC final rule?

Key Deadlines

- **November 2, 2020** — Information blocking prohibitions, but only with respect to electronic health information (EHI) represented by the data elements in the USCDI standard.
- **May 2, 2022** — Information blocking prohibitions apply to full EHI.
- **May 1, 2022, Enforceable August 1, 2022** — Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR) application programming interface (API) capability.

Patient Access to Information

ONC finalized a new requirement that requires health IT developers (e.g., an EHR vendor) of ONC Certified Health IT to develop "certified API technology" for API information sources (e.g., a hospital using the vendor's EHR) that will allow health information from such technology to be accessed, exchanged, and used without special effort on the part of the API user (app developer). This new certification criterion, along with associated conditions and maintenance of certification requirements, will allow both patients and providers to use apps to connect to the certified API technology to access information. In a parallel policy, ONC also requires providers to make such standardized web-based technology available.

Required Data Elements

Providers mut make available standardized API access for single patient and population services. The technology must include API-enabled "read" services using the FHIR standard, meaning it does not need to be bi-directional or "read and write." For both single and population services, the API technology will be required to respond to requests for data specified in the USCDI.

Required Standards

The technical standards for this certification criterion including documentation, app registration, security, authentication and authorization requirements, are the same as those outlined in the CMS rule. Note, CMS does not require health insurance provider APIs to get certified through the ONC process like Certified Health IT, but largely applies the same requirements.

Certified API Developers are permitted to charge fees to API information sources for the development, deployment, and upgrade of their certified API technology, and towards recovering API usage costs. Developers are also permitted to charge API users for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy the app. All other fees are prohibited.

Certified Electronic Health Record Technology (CEHRT). The ONC Health IT Certification program is a voluntary program established in 2010 to certify health IT used in federal, state, and private programs. Requirements for certification are established through standards, implementation specifications and certification criteria adopted by the Secretary.

Information blocking is any practice that is likely to interfere with access, exchange, or use of electronic health information (except as required by law or covered by an exception to the provision); and

- If conducted by a *health information technology developer, health information network or health information exchange,* such developer, network or exchange knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; or
- If conducted by a *health care provider,* such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Information blocking actor means a health care provider, health IT developer of certified health IT, health information network or health information exchange. Only information blocking actors are subject to the information blocking provision. For detailed descriptions of each of the actor types, please see the ONC website here.

Information Blocking

Information blocking is any practice that is likely to interfere with access, exchange, or use of electronic health information. Through this rule, ONC seeks to broaden both those entities and data subject to information blocking penalties.

Before May 1, 2022, EHI for purposes of the information blocking provision is defined by the data elements represented in the USCDI standard. From May 2, 2022, onwards, EHI for purposes of the information blocking provision means electronic protected health information as defined for HIPAA, regardless of whether the group of records are used or maintained by or for a HIPAA-covered entity.

Information blocking "actors" include health care providers and health IT developers, and Health Information Network (HIN)/Health Information Exchanges (HIE). The final rule combines the definitions of HIN and HIE to create one definition that applies to both statutory terms and specifies that to be a HIN/HIE, there must be more than two unaffiliated individuals or entities besides the HIN/HIE that are enabled to exchange with each other. While ONC adopted a modified definition of HIN/HIE to address much of the feedback received during public comment, they declined to expressly exclude any specific type of entity from the definition leaving in question whether it may be applicable to health insurance providers.

The ONC identifies eight categories of practices that, provided certain conditions are met, would not constitute information blocking and, thus, would not subject the actor to civil penalties or other disincentives under the law.

Exceptions that involve not fulfilling requests to access, exchange, or use EHI include:

- Preventing Harm Exception
- Privacy Exception
- Security Exception
- Infeasibility Exception
- Health IT Performance Exception.

Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI include:

- Content and Manner Exception
- Fees Exception
- Licensing Exception

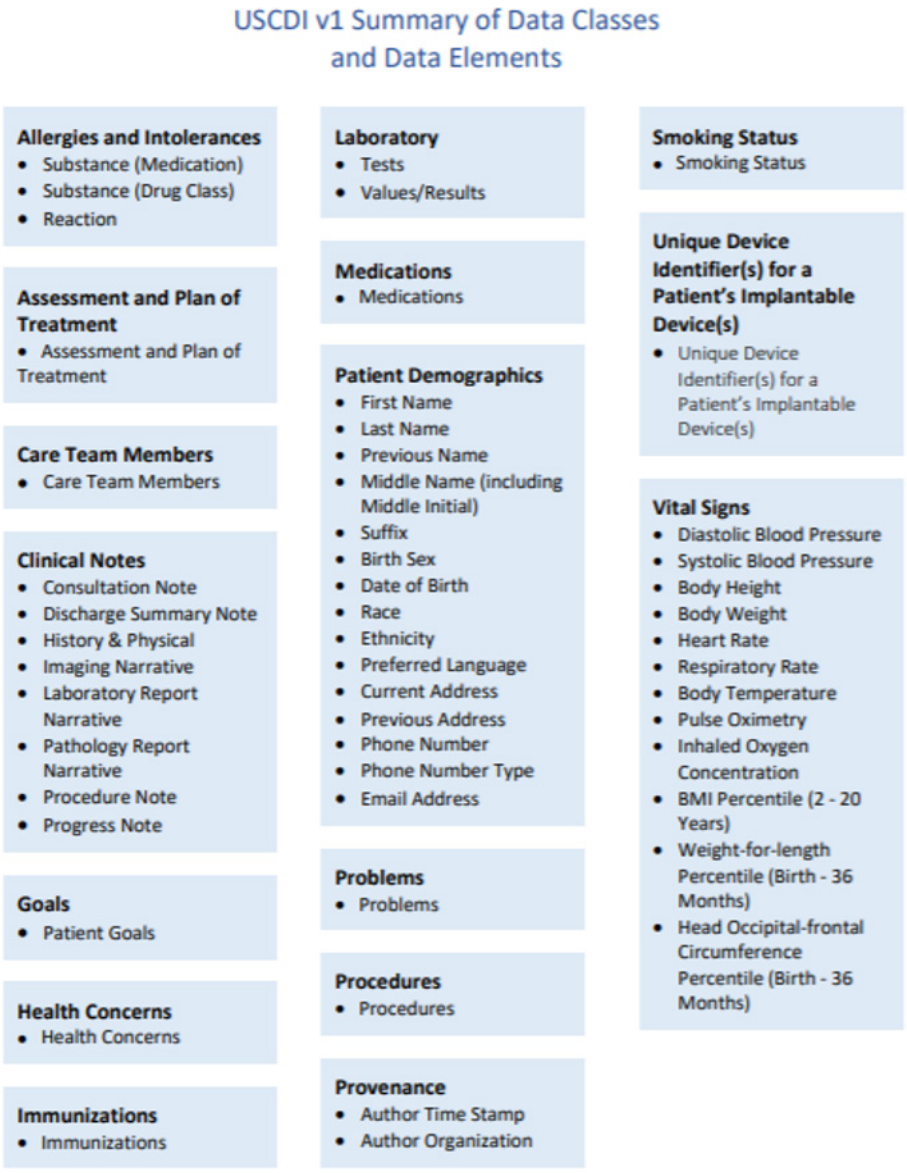
Actors do not have to comply with the information blocking provision until 6 months after publication of the final rule. While health IT developers and HINs/HIEs would be subject to civil monetary penalties (CMPs) for violating the information blocking provisions, health care providers who violate the information blocking provisions would not be subject to CMPs, and instead would be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law. Enforcement of information blocking civil monetary penalties (CMP) of up to $1 million per instance will not begin until established by future notice and comment rulemaking by the Office of the Inspector General (OIG). Actors would not be subject to penalties until CMP rules are final.

Looking forward

In addition to the specific requirements proposed by CMS and ONC and their inherent and ripple effects, we anticipate further development of interoperability policies in the near future based on provisions of these rules that were not finalized and/or pilot programs underway, including:

- Determining the feasibility of providers requesting to **download information on a shared patient population** with a health insurance provider, whether that could be accomplished through a third-party app, and whether it could be done cumulatively to obtain all of a patient's utilization history in a timely comprehensive way;
- Creating further **price transparency** through standards-based APIs;
- Requiring **payer to payer exchange** through standards-based APIs;
- Improving information exchange through standards-based APIs between providers and **registries** to support public health reporting, quality reporting, and care quality improvement;
- Developing a trusted exchange framework and common agreement as well as a network to encourage **care coordination amongst payers,** where payers can choose to participate in a nationwide, secure exchange in data; and
- Allow for a **documentation requirement lookup service (DRLS),** which would enable providers to discover prior authorization and documentation requirements at the time of service through their EHR or integrated practice management system through electronic data exchange with a payer.

Attachment 1: USCDI v1 Summary of Data Classes and Data Elements



What other resources are available?

AHIP slide deck detailing the final rules:

https://www.ahip.org/wp-content/uploads/HealthIT_FinalRuleSlides_3_18_20-v1.pdf

AHIP podcast by AHIP staff giving a detailed summary of the rules (audio and slides):

https://www.ahip.org/member-resources-for-chief-medical-officers/

HHS Press Release:

https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html

CMS Fact Sheet:

https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet

CMS Final Rule:

https://www.cms.gov/files/document/cms-9115-f.pdf

ONC Final Rule:

https://www.healthit.gov/sites/default/files/cures/2020-03/ONC_Cures_Act_Final_Rule_03092020.pdf

Standards:

- HL7 FHIR standard https://www.hl7.org/fhir/overview.html
- USCDI Version 1 standard https://www.healthit.gov/USCDI
- Open ID Connect https://openid.net/connect/
- OAuth 2.0 https://oauth.net/2/

Blue Button Resources:

- HL7 CARIN Blue Button Implementation Guide: http://hl7.org/fhir/us/carin-bb/2020Feb/
- CARIN Blue Button Framework and Common Payer Consumer Data Set: https://www.carinalliance.com/wp-content/uploads/2018/12/CARIN-Blue-Button-Framework_121018-clean.pdf
- HL7 Implementation Guide proposal: https://confluence.hl7.org/display/FHIR/CARIN+Blue+Button+IG+Proposal
- HL7 Project Page: https://confluence.hl7.org/pages/viewpage.action?pageId=55941223

Have any questions or comments?

For questions on the Rules please contact Danielle Lloyd at dlloyd@ahip.org or 202-778-3246.