CMS and ONC Interoperability Final Rules: Oregon Health Authority's Overview for HITOC

10/1/2020

Disclaimer: The information and dates included below are based on OHA's analysis to date and more information can be found https://www.oregon.gov/oha/HPA/OHIT-HITOC/Pages/Federal-Rules.aspx . *Please refer to the referenced CMS and ONC websites and documents for source information.*

ONC 21st Century Cures Act Final Rule

The Office of the National Coordinator for Health Information Technology (ONC) 21st Century Cures Act Final Rule (Cures Act Final Rule) was published in the Federal Register on May 1, 2020. See ONC Cures Act final rule infographic for regulatory dates and enforcement discretion dates. ONC intends to exercise enforcement discretion for 3 months at the end of certain ONC Health IT Certification Program compliance dates associated with the ONC Cures Act Final Rule to provide flexibility while ensuring the goals of the rule remain on track.

Policy Description	Final Rule Compliance Dates	Considerations and Potential Barriers
1 – ONC: Updates to EHR Certification Criteria The functionality criteria that EHR vendors need to demonstrate in order to become a certified EHR technology (CEHRT) was updated. Providers are required to implement and use CEHRT to participate in several Centers for Medicare & Medicaid Services (CMS) payment incentive and quality reporting programs. Notable certification updates include: • Adoption of the United States Core Data for Interoperability (USCDI): this standard sets the baseline of data classes that should be available for health information exchange	*Update: ONC will exercise enforcement discretion until 3 months after all initial compliance dates.* Vendor compliance: May 1, 2022	Providers must exchange USCDI v1 data elements by November 1, 2020 to avoid information blocking.

Policy Description	Final Rule Compliance Dates	Considerations and Potential Barriers
Notable certification updates include (con't): • Clinical Quality Measures (CQMs) Report: this standard requires health information technology (HIT) modules to support the CMS Quality Reporting Document Architecture (QRDA) Implementation Guide • Electronic Health Information (EHI) Export: new functionality that would allow patients to request an export of their EHI and providers to request an export of all EHI in the EHR • Application Programming Interfaces (APIs): criterion updated to require the use of HL7® Fast Healthcare Interoperability Resources (FHIR®) Release 4	Vendor compliance: July 1, 2020 Vendor compliance: May 1, 2023 Vendor compliance: November 1, 2021	Requires HIT developers to adopt an emerging standard for data exchange. Requires providers to share data with app developers not covered by HIPAA and with no data sharing agreement with the provider.

Policy Description	Final Rule Compliance Dates	Considerations and Potential Barriers
2 – ONC: Exceptions to Information Blocking The rule identifies and outlines eight reasonable and necessary activities that interfere with the access, exchange, or use of EHI, but do not constitute information blocking provided certain conditions are met. The intent is to prevent "information blocking" practices (e.g., anti-competitive behaviors) by healthcare providers, developers of certified health IT, health information exchanges/networks (HIEs/HINs).	November 1, 2020 *Update: ONC will exercise enforcement discretion until 3 months after the initial compliance date* *Update: Office of the Inspector General (OIG) has proposed additional enforcement discretion in OIG's proposed rule for civil money penalties for certified HIT developers, HIEs/HINs yet to be finalized. Provider enforcement TBD in future DHHS rulemaking.*	Payers and healthcare providers should assess whether they have lines of business that function as an HIN and are subject to enforcement deadlines and civil monetary penalties. Requires developers of certified HIT, healthcare providers, and HIEs/HINs to • exchange all (USCDI) v1 data elements, • assess current practices for information blocking and adjust as necessary, and • ensure they utilize widely-accepted and -adopted standards to exchange data. Requires providers to monitor whether their CEHRT vendors have had their certifications revoked as a result of information blocking.

CMS Interoperability and Patient Access Final Rule

The Centers for Medicare & Medicaid Services (CMS) Interoperability and Patient Access final rule was published in the Federal Register on May 1, 2020. CMS finalized seven new policies: four for payers and three for providers.[1] A brief description of each of these topics can be found in the CMS Fact Sheet. On August 14, 2020, CMS released a State Health Official letter that describes how CMS-regulated payers (including Medicaid managed care plans) should implement this final rule. In addition, updated CMS guidance includes adjustments to the implementation and enforcement timeline, technical standards, and implementation guidance for Patient Access and Provider Directory APIs.

[1] Information in this document was taken from CMS' Fact Sheet and other CMS on-line materials and announcements, augmented by OHA analysis.

CMS Interoperability and Patient Access Final Rule: Payer Policies (1-4 of 7 new policies)

Payer policies apply to **CMS-regulated payers only**, which may include (as noted below) Medicare Advantage (MA) organizations, Medicaid Fee-for-Service (FFS) programs, Medicaid managed care plans, Children's Health Insurance Program (CHIP) FFS programs, CHIP managed care entities, and qualified health plan (QHP) issuers on the federally-facilitated exchanges (FFEs), excluding issuers offering only stand-alone dental plans (SADPs) and QHP issuers offering coverage in the federally-facilitated Small Business Health Options Program (FF-SHOP).

Policy Description	Final Rule Compliance Dates and Applicability	Considerations and Potential Barriers
1 of 7 – CMS: Patient Access API CMS-regulated payers are required to implement a specific secure, standards-based API that allows patients to easily access their claims and encounter information, as well as their clinical information through third-party applications of their choosing.	January 1, 2021 *Update: CMS will exercise enforcement discretion for this requirement until July 1, 2021* Applies to MA, Medicaid FFS and managed care, CHIP FFS and managed care, QHPs on FFEs	Requires payers to • budget for system changes, • use standards and terminologies new to existing vendors, • aggregate and map clinical data from existing administrative systems to API standards, • manage patient logins and passwords, • use security standards new to existing vendors, • share Protected Health Information (PHI) with app developers not covered by HIPAA and with no data sharing agreement with the payer, • consider the user experience of the patient, and • provide patient education on 3rd party app privacy (see CMS resource)

Policy Description	Final Rule Compliance Dates and Applicability	Considerations and Potential Barriers
2 of 7 –CMS: Provider Directory API CMS-regulated payers are required to make provider directory information publicly available via a specific standards-based API. This would include the names of providers, addresses, phone numbers and specialty.	January 1, 2021 *Update: CMS will exercise enforcement discretion for this requirement until July 1, 2021* Applies to MA, Medicaid FFS and managed care, CHIP FFS and managed care	Requires payers to • budget for system changes, • use standards new to existing vendors, • collect any missing provider data, • map provider data from existing administrative transactions to API standards, and • share data with app developers with no data sharing agreement with the payer.
3 of 7 – CMS: Payer-to Payer Data Exchange CMS-regulated payers are required to exchange clinical data specified in the USCDI v1 at the patient's request, allowing the patient to take their information with them as they move from payer to payer over time to help create a cumulative health record with their current payer.	January 1, 2022 *Update: No change* Applies to MA, Medicaid managed care, CHIP managed care, QHPs on FFEs	Requires payers to • budget for system changes, • implement robust beneficiary identity management and patient matching, • use changing data standards and terminologies new to existing vendors, • identify an API standard (none specified in the rule), • implement long-term clinical data retention with on-line access, • create a process for beneficiaries to request information, and • manage patient logins and passwords if part of the request process. • coordinate with other payers

Policy Description	Final Rule Compliance Dates and Applicability	Considerations and Potential Barriers
4 of 7 – CMS: Increased Reporting on Dual Eligibles Each state must implement system changes to support daily exchange of certain enrollee data of individual dually eligible for Medicare and Medicaid with CMS, including state buy-in files and "MMA files".	April 1, 2022 *Update: No change* Applies to Medicaid agencies	Requires payers to • revise processes for more timely updates with CMS, and • coordinate deletions and additions to avoid gaps in dually eligible coverage.

CMS Interoperability and Patient Access Final Rule: Provider Policies (5-7 of 7 new policies)

Provider policies apply to:

- **Hospitals**: eligible hospitals (EH), short-term acute care, long-term care, rehabilitation, psychiatric, children's, cancer hospitals, and critical access hospitals (CAHs); includes the hospital Promoting Interoperability (PI) Program
- **Clinicians**: physicians and eligible clinicians (EC); includes the Quality Payment Program (QPP)

Policy Description	Final Rule Compliance Dates	Considerations and Potential Barriers
5 of 7 – CMS: Public Reporting and Information Blocking CMS will publicly report eligible clinicians, hospitals, and critical access hospitals (CAHs) that may be involved in information blocking based on how they attested to the CMS Promoting Interoperability (PI) Program or CMS Merit-based incentive payment system (MIPS).	Applicable late 2020	Providers should review and update their attestations as appropriate. States may want to consider and review their role in educating providers on this requirement.
6 of 7 – CMS: Digital Contact Information CMS will begin publicly reporting those providers who do not list or update their digital contact information in the National Plan and Provider Enumeration System (NPPES).	Applicable late 2020	Requires providers to • know their current digital contact information, • remain aware of changes to digital contact information, and • develop processes to actively update their NPPES information. Some providers may be concerned about abuse when making Direct messaging addresses publicly available.

Policy Description	Final Rule Compliance Dates	Considerations and Potential Barriers
7 of 7 – CMS: Admission, Discharge, and Transfer (ADT) Event Notifications CMS is modifying their 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.	Applicable May 1, 2021 Applies to hospitals only	Requires hospitals to • identify appropriate recipients of notifications (primary care provider, primary care practice group, others identified by the patient), • modify registration processes to identity and record recipients, • create interfaces to primary care recipients or a 3rd party (e.g., HIE) as necessary, perhaps translate notifications to another method for providers unable to receive ADTs, and • modify existing ADT messages as necessary. The CoP process may be ill-equipped to assess fulfillment of this requirement. This requirement puts hospital participation in Medicare at risk.