Summary of the Centers for Medicare & Medicaid Services' (CMS) Interoperability and Patient Access Final Regulation

Table of Contents

I. Overview

On May 1, 2020 (effective date June 30, 2020), CMS published a final regulation aiming to improve patient access to and electronic exchange of claims data. The final regulation, titled Interoperability and Patient Access, is designed for payers who contract with the Agency (e.g., Medicare Advantage, Medicaid, CHIP, and Qualified Health Plan issuers on the Federally Facilitated Exchanges). CMS calls for payers to use the same standards-based APIs that ONC outlines for the vendor community in their rule. The goals of the CMS regulation are to improve patient access to data held by payers as well as exchange of electronic health information between payers.

II. Key Takeaways and Implications

a. ACP Supports

Electronic Admission, Discharge, and Transfer (ADT) notifications: ADT notifications provide the opportunity to provide useful information to clinicians regarding their patient population as they enter and move through various healthcare settings. However, these notifications have the potential to be a new burden if not presented in meaningful and actionable ways.

Updates to "Provider" Directory and Digital Contact Information: Support CMS efforts to update "provider" directory information and digital contact information.

b. ACP'S Remaining Concerns

Privacy of electronic health data: As with the ONC regulation, the College remains concerned around the underlying privacy policy issues regarding increased access to patient data via third-party apps – as well as increased access by insurers and potential for negative coverage determinations or physician contracting terms based on clinical data that was not previously accessible.

Development and Implementation Timelines: There are still a number of varying compliance and implementation deadlines, and we remain concerned about when the technical upgrades will be ready versus when the upgrades will be required for use.

III. Summary of Key Provisions in CMS Final Rule

a. Patient Access Application Programming Interfaces (APIs)

Medicare Advantage plans, Medicaid and Children's Health Insurance Program (CHIP) managed care plans, state agencies, and Qualified Health Plan (QHP) issuers on Federally Facilitated Exchanges ("payers") are required to implement and maintain an API to support patient access to their health information (the "Patient Access API").

Note: CMS provides no specific requirements or guidance concerning information sharing between payers and clinicians through APIs.

Standards and Technical Requirements

- The API must be compliant with the HL7 FHIR Release 4.0.1 standard and the health plans' obligations under the HIPAA Privacy Rule. The rule is intended to have CMS Payers use functionalities similar to CMS' Blue Button 2.0 model that allows patients, their representatives, and any third-party apps designated by such patients and representatives (collectively, "Requestors"), to access claims and encounter information (including approved or denied adjudicated claims, encounters with capitated clinicians, clinician remittances, enrollee cost-sharing), and all clinical data, including laboratory results and medication information (if maintained by the CMS Payer).
- CMS proposes to make publicly accessible documentation that includes, at a minimum:
    - API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns;
    - The software components and configurations an application must use in order to successfully interact with the API and process its response(s); and
    - All applicable technical requirements and attributes necessary for an application to be registered with any authorization server(s) deployed in conjunction with the API.
- Payers, clinicians, and patients cannot direct specific segments of data be made available via this Patient Access API. CMS says that the required data segmentation standards are not widely adopted.

Data Availability

- Payers must make data available through the Patient Access API no later than one (1) business day after claims processing or encountering data receipt.
- Payers must make available through the Patient Access API data that they maintain with a date of service on or after January 1, 2016. This means that no information with a date of service earlier than January 1, 2016, will need to be made available through the Patient Access API. "Date of service" means the date the patient received the item or service, regardless of when it was paid for or ordered.
- The rule specifically limits the obligation to make clinical data available through the Patient Access API to those payers that maintain any such data.
- In order to encourage clinicians to make clinical data available in as timely a fashion as possible, CMS suggests that payers add language to contracts that specify timelines for sharing data.
- "Provider" directory data will not be supplied through the Patient Access API. Instead, CMS specifies the use of a separate "Provider" API.

Privacy and Security – Payer Vetting of Third-Party Apps

- The only instance per the policies proposed in this rule that would allow a payer to deny access to an app would be if the covered entity or its business associate's own systems would be endangered if it were to engage with a specific third-party application through an API. For instance, if allowing such access would result in an unacceptable security risk.
- Covered entities and business associates are free to offer advice to patients on the potential risks involved with requesting data transfers to an application or entity not covered by HIPAA, but such efforts generally must stop at education and awareness or advice regarding concerns related to a specific app.
- Once these data are received by a third-party and no longer under the control of the covered entity or its business associate, the covered entity and business associate are not liable for the privacy and security of the PHI or any electronic health information sent.
- CMS will be providing payers with a framework they can use to request that third-party apps attest to covering certain criteria in their privacy policy, such as information about secondary data use, which payers can use to educate patients about their options.
- The API technical specifications set requirements on the app developer for the app's identity proofing and authentication processes that must be met in order to connect to the API and access the specific patient's data through the API.
- CMS rejected suggestions that it work closely with other HHS agencies and the FTC to establish a transparent regulatory framework for safeguarding the privacy and security of patient electronic health information shared with apps. CMS only agreed to share concerns with other HHS entities.
- Establishing the Patient Access API does not relieve payers of their HIPAA obligations to provide data requested by patients that are not included in US Core Data for Interoperability (USCDI). Any HIPAA-covered entity would have to share this type of information in a form and format other than the Patient Access API in order to comply with program proposals and in keeping with the HIPAA Privacy Rule right of access.
- Payers are encouraged, but are not required, to request third-party apps attest to having certain privacy and security provisions included in their privacy policy prior to providing the app access to the payer's API. If a payer chooses, they can ask that the apps requesting access to their API with the approval and at the direction of the patient to attest that important provisions that can help keep a patient's data private and secure are in place. If an app has a written privacy policy and does not follow the policies as written, the FTC has authority to intervene.
- On privacy, CMS agrees that it would eliminate some burden from payers and clinicians if they assist with the production of the educational materials needed for the purposes of the requirements in this final rule. As a result, CMS is providing suggested content for educational materials that payers can use to tailor to their patient population and share with patients. Payers must publish on their websites the necessary educational information, but CMS will help supply the content needed to meet this requirement.
- Payers may deny or discontinue any third-party application's connection to their API if the payer reasonably determines, consistent with its security analysis, that allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of protected health information on the payer's systems. The payer must make this determination using objective, verifiable criteria that are applied fairly and consistently across all applications and developers.

- CMS encourages payers to consider setting up functionality to allow patients to view a record of when and with whom their data have been shared via the API.

API Fees

- Payers may pass API costs to patients via increased premiums. In this way, patients could absorb the cost of the API. The costs of "premiums" for MA, Medicaid, and CHIP enrollees are primarily borne by the government, as are some premium costs for enrollees of other programs. CMS claims that the benefits created by the Patient Access API outweigh the costs to patients if payers choose to increase premiums as a result.

b. "Provider" Directory API

Standards and Technical Requirements

- CMS Payers, as already the case for QHPs, will need to implement and maintain a standards-based API conformant with the API technical standards finalized in the ONC Rule (HL7 FHIR Release 4.0.1) to make provider directory information publicly available (the "Provider Directory API").

Information Included for Exchange

- The Provider Directory API must include the CMS Payer's network of contracted providers, including names, addresses, phone numbers, and specialties, updated no later than 30 calendar days after providers update their information with the plan.
- Medicare Advantage organizations offering Part D plans must also offer the number, mix, and addresses of pharmacies in their networks. It is expected that third-party application developers will primarily use these APIs.

c. Payer-to-Payer Data Exchange

CMS Payers must comply with patients' requests to send their clinical data, inclusive of the elements defined in the USCDI version 1 data set, to other CMS Payers, to ensure that the new payer has patients' complete records if they change plans.

United States Core Data for Interoperability (USCDI) v1

- USCDI version 1 includes high-level clinical data including allergies, clinical notes, patient goals and health concerns, immunizations, laboratory tests and results, medications, procedures, and vital signs.
- The USCDI standard aligns with the ONC Rule's definition and exceptions for information blocking and the same API standard for exchanging patients' electronic health information.

d. Trusted Exchange Network Requirements

CMS proposed to require plans to participate in trust networks in order to improve interoperability in these programs. CMS has chosen not to include this requirement in the final rule.

e. Dual Eligible Coordination

State agencies will be required to exchange Medicare and Medicaid dual enrollee data on a daily basis with CMS. Currently states are only required to exchange this data on a monthly basis.

f. Public Reporting of Information Blocking Practices and Noncompliance with Digital Contact Information Requirements

CMS will publicly list clinicians, hospitals, and CAHs that are determined to be engaged in information blocking based on information disclosed by such clinicians and entities as part of the "Promoting Interoperability" reporting requirements imposed under CMS's Quality Payment Program (QPP). The Agency will also publicly report such entities that do not list or update their digital contact information in the National Plan and "Provider" Enumeration System (NPPES). Digital contact information is intended to include secure digital endpoints like a Direct Address or FHIR API endpoint where USCDI-compliant data would be received from or sent at a patient's request. Public reporting related to the information blocking requirements will be included on the Medicare Physician Compare website, but CMS has not finalized where public reporting related to digital contact information will be placed.

g. Admission, Discharge, and Transfer (ADT) Notifications

CMS's Medicare Conditions of Participation (CoPs) for hospitals and critical access hospitals (CAHs) will require that they send electronic patient ADT event notifications to other health care facilities or community clinicians (including primary care practitioners or practice group, or post-acute services clinicians). In contrast to the proposed rule, this requirement includes event notification requirements for any patient who accesses services in hospital emergency departments or any inpatient hospital services.

Required Data within ADT Notification

- Patient's name, the treating provider's name, and sending institution's name, sent electronically directly or through a health information exchange or health information network, to the patient's primary care provider/practice, applicable post-acute care provider, or any other provider identified by the patient.
- CMS did not include the proposed requirement that the notifications include diagnosis information, although hospitals may decide to include diagnosis or additional information beyond the minimum required.

IV. Timelines

- **May 1, 2020** – Final regulations published in Federal Register

- **Late 2020**
  - CMS will publicly list those determined to be information blockers
  - Digital Contact Information requirements

- **January 1, 2021**
  - Medicare Payers must implement and maintain an API to support patient access to data (**enforcement discretion through July 1, 2021**)
  - Medicare Payers must implement and maintain an API to make provider directory information publicly available (**enforcement discretion through July 1, 2021**)
  - Qualified Health Plan insurers on Exchanges must implement and maintain API to support patient access (**enforcement discretion through July 1, 2021**)

- **May 1, 2021 –** 12 months after FR publication
  - Hospitals required to have ADT notifications implemented as part of their Medicare Conditions of Participation

- **January 1, 2022**
  - Payer-to-Payer exchange: CMS Payers must comply with patients' requests to send their clinical data, inclusive of the elements defined in the USCDI version 1 data set, to other CMS Payers, to ensure that the new payer has patients' complete records if they change plans

- **April 1, 2022**
  - Dual Eligible Coordination – state agencies required to exchange Medicare and Medicaid dual enrollee data on a daily basis