CMS Interoperability and Patient Access Final Rule

David S. Szabo, Boston

Massachusetts Health Data Consortium CIO Forum

Stated Goal

This final rule is intended to move the health care ecosystem in the direction of interoperability, and to signal our commitment to the vision set out in the 21st Century Cures Act and Executive Order 13813 to improve the quality and accessibility of information that Americans need to make informed health care decisions, including information about prices and outcomes, while minimizing reporting burdens on affected health care providers and payers.

Background

Proposed Rule published March 4, 2019.

Numerous comments

First Phase of policies focusing on interoperability and patient access to their own information

Coordinates with other rules and initiatives, such as the Information Blocking Rule

Who Does it Apply to?

In general, Medicare and Medicaid programs (including MA Plans and Medicaid MCOs)

CHIP

Qualified health plan issuers on the individual market Federally-Facilitated Exchanges

Excludes:

Plans on state-based exchanges

Stand alone dental plans

Small Business Options Program Exchanges.

Overview of Goals

Facilitate longitudinal view of patient health data and services rendered:

Increase access for pharmaceutical companies, device manufacturers, and payors to health data;

Facilitate transitions of care;

Facilitate transition between payors and benefits coordination; and

Empower patients to make decisions to support better outcomes.

MyHealthEData Initiative

Key policies embedded in the Final Rule:

- Enable access by patients to their data requiring payors to make data available through an API to which third-party applications may connect;
- Ensuring access by providers to data about care previously received by their patients from other providers;
- Requiring the payors make information about their enrollees available with the use of software to be developed by payors and third parties such that data is available to the enrollees for use by providers, social service providers and other payors; and
- Improve availability to current and prospective enrollees about provider networks.

Barriers to Interoperability

Patient Identification.

Lack of standardization.

Information Blocking.

Lack of Certified HIT among Post-acute providers.

Privacy concerns and uncertainty about HIPAA Rules.

CMS: “We believe there is still considerable work to be done to overcome some of these challenges . . .”

Patient Access API

MA Plans, Medicaid, CHIP FFS and managed care plans, Medicaid MCOs and federal-exchange QHPs must maintain a standards-based Patient Access API.

Standards are HL7 FHIR using content and vocabulary standards approved by HHS under 21st Century Cures Act.

Payors must permit third-party applications that comply with the standards to retrieve certain data **as directed by the enrollee.**

Data includes adjudicated claims (including cost sharing); encounters with capitated providers; and clinical data, including lab results, if maintained by the payor.

Applies to dates of service on and after January 1, 2016.

Patient Access API (contd.)

CMS has very high expectations for the Patient Access API in terms of improving care and outcomes.

Patient Access API **does not replace HIPAA rules** on access to data held by a covered entity or business associate.

No special funding source to support costs, but cost should be part of premium calculation for Medicare Advantage and Medicaid MCO plans. CMS will provide a 90% match rate for FSS Medicaid.

CMS does not require a centralized data hub for all payers or require the use of portals. CMS is requiring payers to “unleash their data.”

Patient Access API (contd.)

CMS received comments objecting to the inclusion of claims information that might disclose amounts paid for specific services. Some commenters requested that CMS prohibit third-party apps from aggregating claims data for any purpose other than disclosure to the patients who received the services.

CMS responded that *"the benefits of making this information available to patients through third-party apps outweighs these concerns . . . there is a chance the app could aggregate or otherwise analyze the data, assuming the single app has access to enough patient data in a given market or patients who use a particular payer or plan, to make such an analysis possible. Appreciating patients already have access to this information and understanding the possibility for secondary uses of such data, we are finalizing the policy as proposed to require plans to share adjudicated claims, including provider remittances and enrollee cost-sharing information."*

Patient Access API (contd.)

Directory data does need to be included via the Patient Access API, as there is a separate provision of the rule for this this information.

Clinical data, to the extent maintained by the payer, should follow the content and vocabulary of the United States Core Data for Interoperability (USDC).

Payors subject to the rule cannot charge a fee to third-party app developers for accessing the Patient Access API. Documentation concerning APIs also must be available without charge. Payers are permitted and required to implement security safeguards to authenticate that the data is being released at the request of a particular member and to protect their own systems.

Provider Directory API

MA Plans, Medicaid, CHIP FFS and managed care plans, Medicaid MCOs and federal-exchange QHPs also must make standardized information about their provider networks available through a Provider Directory API, based on the technical standards approved in the 21st Century Cures Act regulations, **excluding the user authentication and authorization protocols.**

The API must be available via a public-facing digital endpoint on the payer's website to as to promote public access to the directory information.

The directory information must include provider name, address, phone number and specialty. MA organizations that include Part D coverage must include pharmacies.

This requirement must be fully implemented by January 1, 2021.

Payer-to-Payer Data Exchange

MA Plans, Medicaid, CHIP FFS and managed care plans, Medicaid MCOs and federal-exchange QHPs must coordinate care with other payors by exchanging data for all dates of service on or after January 1, 2016, **at the enrollee's request.** This data must include at a minimum, the data elements specified in the United States Core Data for Interoperability version 1.

USDCI consists of clinical, demographic and provenance information. Unlike the Patient API, it does not include paid claims information.

CMS did not adopt an standards-based API requirement or HIE requirement for Payer-to-Payer exchange, but stay tuned in the future.

Payer-to-payer data exchange must be implemented by January 1, 2022.

State Exchange of Buy-In Data for Dual-Eligibles

The States and territories that participate in Medicaid must participate in daily exchange of buy-in data, which includes sending data to CMS and receiving responses from CMS.

This must be implemented by April 1, 2022.

This rule is expected to improve the ability of payors and providers to coordinate eligibility, enrollment, benefits and care for dually-eligible patients.

Physician Compare and Hospital Data and Information Blocking

Physician Compare data will include an indicator for clinicians and groups that submit a “no” response to any of the three statements relating to information blocking that is submitted for MIPS.

A similar indicator will be established for hospitals on the CMS website.

This information will be relate to attestations and responses staring in 2019, and will be posted by CMS in late 2020.

Note: Information Blocking sanctions are already incorporated into MIPs and into existing regulations adopted under 21st Century Cures Act.

Digital Contact Information

CMS will publicly-report providers, by name and NPI, who do not have digital contact information included in the NPPES system. CMS also will encourage providers to include their digital contact information in their FHIR endpoint, as well.

Hospital COPs and Event Notification

Medicare and Medicaid safety standards will be amended to promote data exchange to support transitions of care.

Hospitals, psychiatric hospitals and critical access hospitals that utilize an electronic medical record system that conforms to the content exchange standard are required to demonstrate that their system's notification capacity is fully operational.

Those systems are required to send Admission, Discharge and Treatment (ADT) notifications that include the patient name, treating practitioner and sending institution's name. A diagnosis should be included if permitted by law.

Hospital COPs (contd.)

Notices should be send:

- Upon registration in the emergency department;
- Admission to an inpatient service;
- Discharge or transfer from the emergency department; and
- Discharge or transfer from inpatient services.

Hospitals are required to make a “reasonable effort” to send ADTs to applicable post acute provider and suppliers, the patients PCP or other practitioner or group practice identified by the patient.

Hospital COPs (contd.)

The hospital can send notifications either directly or through an health information exchange organization. The final rule does not mandate any new standards for ADT-based notifications, and it does not bar hospitals from including additional information in the notifications.

The rule does not change or waive any existing privacy regulations. CMS assumes that ADT-notifications will comply with all other applicable law, i.e., HIPAA and state privacy laws.

This requirement is effective six months after publication of the rule.

Technical Standards Adopted

CMS uses the definition of interoperability from Public Health Services Act as amended by 21st Century Cures Act:

> Information technology is interoperable if it enables the secure exchange of electronic health information from other systems without special effort on the part of the user, allows for complete access, exchange and use of all electronic health information permitted under applicable law, and does not constitute information blocking

CMS does not consider portals tethered to EHRs or propriety systems developed by payors and providers as meeting this definition.

CMS views the rule as an extension of the Blue Button 2.0 initiative that makes claims and encounter data available to Medicare beneficiaries.

Technical Standards (contd.)

CMS comments on standards-based APIs:

- Current standard is Health Level 7® (HL7) Fast Healthcare Interoperability Resources® (FHIR) Release 4.0.1/
- Standards for APIs include security safeguards (open does not mean insecure);
- The API technology is standardized, along with the content and vocabulary to be transmitted and received (e.g. USCDI v.1);
- APIs must be technically transparent; and
- APIs must be implemented in a pro-competitive manner (i.e. efficiency enhancing and not excluding competitors).

Regulated entities are precluded from using non-standard APIs for the purposes set out in the Rule, including prior versions of currently effective standards.

Privacy and Security Concerns

CMS received many comments related to privacy and security.

HIPAA requires CEs and BAs to protect their own systems and data when using Standard APIs, and to take reasonable safeguards to protect ePHI in transit. The Final Rule does not alter HIPAA in any respect.

CMS clarifies that CEs and BAs **are not responsible** for the security of ePHI once it has been transmitted to a third party application chosen by the patient or the patient's legal representative.

The Federal Trade Commission has authority to regulate non-healthcare parties that receive PHI. These entities may be subject to the FTC's Health Breach Notification Rule

Payors will be required to provide guidance to enrollees about selecting third-party applications, protecting PHI and filing complaints.

Privacy and Security Concerns

Covered Entities and their BAs may deny access to a third-party application if their own systems would be endangered if it were to engage with a specific application.

Absent such a concern, Covered Entities may only advise patients or enrollees of the risks posed by third party recipients (e.g. to notify the individual to review the privacy policy of the third party). However, absent a security risk to the sender, the CE or BA must follow the individual patient's directive.

CMS notes that APIs are subject to technical requirements regarding user authentication, app authentication and identity proofing.

Blue Button 2.0 consumer guidance can be used by payors, but is not required *per se*.

Brave New World

Enrollee's will exercise their rights of access to the Patient Access API and the Directory API through third-party app developers.

If app developers work under contract with payers or providers, they could end up being business associates, subject to HIPAA privacy and security rules.

CMS contemplates that most app developers will be independent of payers and providers, and will be primarily regulated by the Federal Trade Commission.

Potential issues: secondary uses of ePHI outside of HIPAA; aggregation of paid claims data outside of HIPAA or other direct regulation; sales of ePHI, and others yet to be identified.

Brave New World

App developers eventually will show up with connection requests on behalf of enrollees. Plans must be prepared to authenticate requests and implement safeguards to weed out inappropriate requests and protect their own systems.

Providing “guidance” to enrollees on the selection of third-party apps could be challenging.

See https://www.medicare.gov/manage-your-health/medicares-blue-button-blue-button-20/blue-button-apps

https://bluebutton.cms.gov/blog/How-Beneficiaries-Authorize-an-App.html

CMS has opened the door to data releases but has not fully thought through the consequences.

Summary

Type of Exchange	Minimum Required Data	Time frame	Deadline
Patient API, Allows Patient to Pull Data from Payor via Third-Party App.	Claims and encounter data, clinical data to the extent maintained by payer, including data received from predecessor Payer.	January 1, 2016 and after	January 1, 2021
Directory API, Allows Anyone to Pull Provider Directory Data from Payor	Provider names, addresses, phone numbers and specialties. MA organizations with Part D must include pharmacy names, address phone number, the number of pharmacies in the network and types.	Update within thirty days of any change or update.	January 1, 2021
Payor to Payor at the direction of the enrollee	At least USDCI version 1 clinical data as maintained by payor	January 1, 2016 and after	January 1, 2022
Coordination of Benefits for Dual Eligible Patients	Record of each Medicare beneficiary for who the state is paying Medicare premiums, plus exchanges of demographic data	Daily	April 1, 2022
Hospital ADT messages to physicians and post-acute facilities	Admission to ED or inpatient service and discharges from ED or inpatient service	As occurring	Six months after publication of the rule.

Questions?

David S. Szabo

Locke Lord LLP

David.Szabo@lockelord.com

617-239-0414

ATTORNEY ADVERTISING. Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This presentation is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice.