A Primer for Medicaid/CHIP State Agencies on the Patient Access API Requirement of the CMS Interoperability and Patient Access Final Rule (CMS-9115-F)

The Final Rule was published in the Federal Register on May 1, 2020 and can be found at: https://www.federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and

What is the Purpose of the Rule?

- To provide patients:
  - access to a cumulative record of their health information across payers; and
  - the ability to decide how their data will be used, while keeping that information safe and secure.
- To move the healthcare system toward greater interoperability.

Who does the Rule Impact?

- Medicaid and CHIP Programs
- Medicaid and CHIP Managed Care Organizations, including Pre-paid Inpatient Health Plans and Pre-paid Ambulatory Health Plans
- Medicare Advantage Plans
- Qualified Health Plans on the Federal Exchange

What does the Rule Require State Medicaid/CHIP Agencies to do?

1. Implement and Maintain a Patient Access Application Programming Interface (API)
2. Implement and Maintain a Provider Directory API
3. Increase the Frequency of Federal-State Data Exchanges for individuals eligible for Medicaid and Medicare
4. Require, through contracts, that Medicaid Managed Care entities comply with the Rule.

Patient Access API

In order to comply with the Patient Access API requirements of the Final Rule, Medicaid/CHIP State agencies must enable current Medicaid/CHIP eligible individuals **to access their claims data[1] electronically through third party applications of their choice.**

Once these requirements are implemented, a Medicaid/CHIP eligible individual should be able to download an app and direct that app to access and download their data from the Medicaid/CHIP State agency. The individual can then share this data with other family members, care-givers, providers or use the data in any way the individual decides. The Final Rule is focused on providing individuals access and use of their health information.

This brief summarizes the action steps Medicaid/CHIP State agencies need to take to comply with the Patient Access API section of the Final Rule:

1. **Ensure the Appropriate Data is Ready to Transmit**
2. **Communicating with App Developers**
3. **Communicating with and ensuring Privacy and Security for Medicaid/CHIP eligible Individuals**
4. **Implementation Timeframe and Considerations**

What is an API?

The **Office of National Coordinator (ONC)** defines APIs as "messengers or translators that work behind the scenes to help software programs communicate with one another."

Think about searching for a flight. Before APIs, people had to visit various airlines' websites to compare prices. Now, there are travel search programs that centralize airline flight information. How do they do this? By using APIs.[1]

[1] If the Medicaid/CHIP State Agency maintains specific clinical data, such as laboratory results, that data will need to be available as well.

Steps to Implementing the Patient Access API

Strategy

Given the short timeframe for implementation, Medicaid/CHIP State agencies will be motivated to focus on procurement and technical considerations. It is important that time be taken to develop an overall strategy for this new business process. At least two aspects will be new for most agencies.

The first is the ability for individuals to easily access data about their health care utilization. Several Medicaid/CHIP State agencies plan to employ the requirements of this Rule in an overall effort to engage Medicaid beneficiaries in a different way -whether that is more mobile engagement or a general change in customer-oriented processes. This is a new service that agencies will be able to provide. It has the potential to significantly change how the agency interacts with the people it serves. Implementation of this Rule will impact the agency far beyond its technology. Several operational questions will need to be considered. For example, if a Medicaid/CHIP eligible individual finds data is not correct, is there a process to address the error?

Agencies are urged to consider this Rule as a first step in moving towards more interoperability and to think about the positive impact it can have on the people and families served. For example, Medicaid/CHIP State agencies might consider opportunities the Final Rule could provide for people with intellectual/developmental disabilities or physical disabilities, communities for which access to integrated data has been particularly challenging.

The second new aspect is the use of Application Programming Interfaces (APIs). For some agencies, this may be the first time APIs will be used to transmit and share data. Agencies are encouraged to explore whether the use of APIs in other aspects of their technical approach makes sense.

1. Ensure the Appropriate Data is Ready to Transmit

1.a. Identify the Data to Transmit through the API

The information that will be transmitted needs to include, at a minimum:

- Adjudicated claims, appealed payment decisions, provider remittances, including enrollee cost sharing; within (1) business day after the claim is processed.

- This includes claims for long-term services and supports; transportation; durable medical equipment; dental visits. In summary, any claim paid on behalf of the individual should be included.

- Encounter data that a State pays directly; within (1) business day after the encounter is received.

Encounter Data

Medicaid/CHIP beneficiaries should not be receiving information from both the state and managed care plan for the same service.

Each Payer is only responsible for transmitting data for claims for which it maintains or is directly responsible. If a Medicaid/CHIP State Agency contracts with Managed Care Organizations (MCOs), it is not responsible for transmitting MCO encounter data. If you do not have the data, you do not need to share it.

- Clinical data, such as laboratory results, (when maintained by the State Medicaid agency); within (1) business day after the encounter is received

- Outpatient drug information such as current formularies and preferred drug lists

The final Rule defines ‘‘maintain’’ to mean the payer has access to the data, control over the data, and authority to make the data available through the API.[2]

Claims, encounters, and clinical data with dates of service **on or after January 1, 2016** should be transmitted. 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’’ is the date the patient received the item or service, regardless of when it was paid for or ordered.

Medicaid/CHIP State agencies need to maintain and make available data from January 1, 2016 on for current Medicaid/CHIP eligible individuals. The Patient Access API is only required for current beneficiaries. Once an individual is no longer Medicaid-eligible, the Medicaid/CHIP State agency no

[2] 85 FR 25538

longer needs to make their claims/encounter/clinical data available to them via the Patient Access API.

1.b. Prepare the Data to Transmit through the API

CMS issued the Final Rule at the same time as the Office of National Coordinator (ONC) issued their 21st Century Cures Act final rule.[3] The standards that CMS is requiring Payers, including Medicaid/CHIP State agencies, to meet are set by ONC and consistent with standards set for private payers.

The Final Rule requires Medicaid/CHIP States agencies to ensure the data and the exchange of that data meet specific content and technical standards set by the ONC at 45 CFR §170.213 and §170.215.

Those regulations require that the API meet the **HL7® FHIR Release 4.0.1** standard. **Health Level 7®** (HL7) is an organization that develops standards for the exchange, integration, sharing, and retrieval of electronic health information.[4] They have developed the Fast Healthcare Interoperability Resources (FHIR) standard to "facilitate the exchange of healthcare information between healthcare providers, patients, caregivers, payers, researchers, and anyone else involved in the healthcare ecosystem." The ONC Fact Sheet, *What Is FHIR®?* explains that the **HL7® FHIR®** standard defines how healthcare information can be exchanged between different computer systems regardless of how it is stored in those systems.[5]

The CMS Final Rule recommends the use of several implementation guides. **HL7®** defines implementation guides as, "a set of rules about how FHIR resources are used (or should be used) to solve a particular problem, with associated documentation to support and clarify the usage."

For claims/encounter data, CMS suggests using the CARIN Alliance CPCDS Implementation Guide (IG) (http://hl7.org/fhir/us/carin-bb/history.html).

Any clinical data that the Medicaid/CHIP State agency maintains must be in the form of the United States Core Data for Interoperability (USCDI) version 1 and implementation should use either the US Core IG

[3] https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification
[4] http://www.hl7.org/
[5] https://www.healthit.gov/topic/standards-technology/standards/fhir-fact-sheets

(https://hl7.org/fhir/us/core/history.html) or the PDex IG (https://hl7.org/fhir/us/davinci-pdex/history.html). You can find out more about these different options at: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

A complete list of IGs and additional resources can be found here: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

2. Communicating with App Developers

2.a. Ensure Application Developers Understand how to Connect to the API

Medicaid/CHIP State agencies will need to consider how they will manage communications with the developer community.

The CMS Final Rule includes the minimum information that Medicaid/CHIP State agencies need to provide to developers. Agencies should consider how to **actively engage with developers**. The goal of the Rule is that Medicaid/CHIP beneficiaries take advantage of the ability to access their data; this requires that developers build the apps that will enable the data to be provided. Agencies can ensure apps meet the needs of Medicaid/CHIP eligible individuals through use cases and other helpful information.

While the Final Rule does not explicitly require that Medicaid/CHIP State agencies establish a Developer Portal, there should exist a mechanism that enables third party app developers to learn how to connect to your agency's API.

At a minimum, the following information needs to be available to app developers: [6]

- 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

[6] 85 FR 25543

- All applicable technical requirements and attributes necessary for an application to be registered with any authorization server(s) deployed in conjunction with the API.

2.b. Maintain the API

Once the API is implemented, it must be maintained. The API must be monitored and tested to ensure it is functioning properly. Medicaid/CHIP State agencies should conduct assessments to verify that the API is fully and successfully implementing privacy and security features and is available to third party app developers.

The necessary testing and monitoring should routinely test authentication features that will be used to verify the identity of individual enrollees who seek to access their claims and encounter data and other PHI through the API. Testing will also be needed to ensure the data that is provided is restricted to the requesting individuals data.

Medicaid/CHIP State agencies implementing APIs can incorporate testing tools into a comprehensive testing plan and continuous integration (CI) system, which can automatically validate adherence to the implementation guide (IG) when changes are made. This will mitigate costs associated with testing.

Lastly, Medicaid/CHIP State agencies will need to ensure the API is updated at http://hl7.org/fhir/ .

2.c. Limitations on Ability to Restrict Applications

A Medicaid/CHIP eligible individual can choose to use any third party application that is able to connect to the API maintained by the Medicaid/CHIP State Agency. It is the responsibility of the State Medicaid/CHIP agency to facilitate the connection of those third party applications to the API.

The Final Rule does not change or alter Medicaid/CHIP State agencies' existing responsibilities to protect personal health information (PHI). But the Final Rule does clarify "that covered entities are not responsible under the HIPAA Rules for the security of PHI once it has been received by a third party application chosen by an individual." [7] (emphasis added)

[7] Pg. 25516 of Final Rule (emphasis added)

Medicaid/CHIP State agencies are not responsible for determining whether a third party application "employs appropriate safeguards regarding the information it receives." Medicaid/CHIP State agencies are not required to enter into Business Associate Agreements with the third party application developers.

If a third party application, as a non–covered entity, discloses a Medicaid enrollee or beneficiary's confidential information in a manner or for a purpose not consistent with the privacy notice and terms of use to which the person agreed, the Federal Trade Commission (FTC) has authority to investigate and take action against unfair or deceptive trade practices.

Medicaid/CHIP State agencies must establish **objective, verifiable criteria** that will be applied fairly and consistently across all developers and applications to determine if allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of PHI on the State Medicaid/CHIP systems. If such a risk is discovered, the connection may be denied or discontinued. This is the only instance noted in the Rule in which a Medicaid/CHIP State agency may outright prohibit a third party application from connecting to the API.

3. Communicating with and Ensuring Privacy and Security for Medicaid/CHIP eligible Individuals

For many Medicaid/CHIP State agencies, implementation of this Rule requires re-thinking how the agency interacts with Medicaid/CHIP eligible individuals. For example, the preamble to the Rule encourages (note- this is not required) payers to consider establishing functionality that would allow individuals to view a record of when and with whom their data have been shared via the API. In general, Medicaid/CHIP State Agencies will need to consider if member accounts need to be established, if the agency will need staff to respond to questions about the apps and incorrect data.

What could Medicaid/CHIP eligible individuals do with Claims and Encounter Data?
Based on CMS' experience with Blue Button 2.0:

- Connect with apps that keep track of tests and services they need and receive reminders,
- Track their medical claims, make appointments and send messages to their doctors
- Get personalized information about their symptoms and medical conditions,
- Keep track of their medical notes and questions, and connect to research projects
- Detect and report fraud, waste, and abuse—a critical component of an effective programs.
- Clinicians would be able to review, with the approval and at the direction of the patient, information on the patient's current prescriptions and services received by the patient;
- Clinicians could share data received through the API with the clinician's EHR systems

3.a. Education

Given the limited ability Medicaid/CHIP State agencies have to control third party applications' use of data, the Rule requires agencies to provide resources regarding privacy and security, including information on how current or former Medicaid/CHIP eligible individuals can protect the privacy and security of their health information. These resources must be available through a public website, and communicated in non-technical, simple and easy-to understand language.

CMS is developing information to educate patients about sharing their health information with third parties, and the role of federal partners such as the Office for Civil Rights (OCR) and the FTC in protecting their rights.

3.b. Authentication and Authorization

Any application that accesses a Medicaid/CHIP State Agency's API can only do so with the approval and at the request of a Medicaid/CHIP eligible

individual. State Medicaid/CHIP Agencies need to ensure that consent, authentication, and identity verification processes are sufficient to protect privacy and security. CMS is relying on the security protocols at 45 CFR 170.215 to authenticate users and authorize individuals to access their data. As stated in the Rule's preamble:

> The …"use of **HL7® FHIR Release 4.0.1**, and complementary security and app registration protocols, specifically the SMART Application Launch Implementation Guide (SMART IG) 1.0.0 …and the OpenID Connect Core 1.0 standard…" meets the goal of making "authorization electronic, efficient, and secure so that patients can access their health information as effortlessly as possible."

While the Rule is clear on the standards with which the API and the app developers need to comply, Medicaid/CHIP State agencies will also need to determine how they will authenticate an individual's credentials and if any changes are needed to their existing privacy and security protocols. When a Medicaid/CHIP beneficiary logs onto a third party app, the app will make an API call to the State-designated source to verify that individual's credentials. That source might be the State's eligibility system or the State may need to find an alternative source.

From: Best Practices for Payers and App Developers [8]

Payers required to provide patients their data via the Patient Access API may also ask third-party developers to attest to having certain privacy provisions in place should a patient wish to use the developer's app. For instance, they may ask if the app has a publicly available privacy policy, written in plain language, that has been affirmatively shared with the patient prior to the patient authorizing app access to their health information. When we say "affirmatively shared," we mean that the patient had to take an action to indicate they viewed the privacy policy, such as click or check a box or boxes. Payers can ask if the privacy policy includes important information, such as, at a minimum:

- How a patient's health information may be accessed, exchanged, or used by any person or other entity, including whether the patient's health information may be shared or sold at any time (including in the future);
- A requirement for express consent from a patient before the patient's health information is accessed, exchanged, or used, including receiving express consent before a patient's health information is shared or sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction);
- If the app will access any other information from a patient's device; or
- How a patient can discontinue app access to their data, and what the app's policy and process is for disposing of a patient's data once the patient has withdrawn consent.

[8] https://www.cms.gov/files/document/best-practices-payers-and-app-developers.pdf

4. Implementation Timeframe

As a result of the Public Health Emergency - COVID-19, and to provide additional flexibility to payers, CMS will not enforce these requirements **July 1, 2021**.

Preparation:

- Determine if any State laws exist that might conflict with these requirements.
- Determine Procurement Options for an API and API Management Services:
    - As an amendment or change order to an existing contract
    - As a multi-state purchase through a collaborative such as NASPO ValuePoint
    - In coordination with other Payers in the State
- Participate in Educational Opportunities such as HL7 Connectathons. These are opportunities to test technology and be part of a community working to implement these policies.

APD Submission and Procurement

- Develop and Issue RFP

The Final Rule included assumptions for implementation costs:
On a per Payer basis, the estimates run from a low of $718,414.40, a medium cost of $1,576,829, and a high estimate of $2,365,243.

For a State Medicaid/CHIP agency, DDI would be matched at 90% and Operations at 75%, if approved by CMS.

For Managed Care Organizations, the costs should be recognized in the development of capitation rates.

Design, Development and Implementation

- Determine how to ensure API information is available to potential app developers
- Update public website with Privacy and Security Information
- Outreach to Medicaid eligible individuals