11/5/20 CCO/Payer Federal Interoperability Final Rules Webinar Q & A

This document captures the questions raised at the 11/5/20 CCO/Payer Federal Interoperability Final Rules Webinar and provides responses based on OHA's current understanding of the rules. Given their complexity, additional clarification may be provided in the future. Please visit the CMS and ONC final rules websites for updates and resources. These questions and answers will be compiled with other questions submitted by Oregon stakeholders and posted as FAQs on the Office of Health IT's federal interoperability final rules webpage.

Webinar materials:

- Slides
- Handout
- Webinar audio recording

Oregon Health Authority's Office of Health IT's Interoperability final rules webpage:
https://www.oregon.gov/oha/HPA/OHIT-HITOC/Pages/Federal-Rules.aspx

Webinar agenda

- Webinar Introduction
- Final Rules Overview
- CMS Interoperability and Patient Access Final Rule
- ONC 21st Century Cures Act Final Rule

Webinar Questions & Answers

CMS Interoperability and Patient Access Final Rule: Patient Access API

1. **Regarding the Patient Access API, how should we determine what third party apps we allow users to authenticate through our oauth2 endpoint and then access the API? We would be concerned that untrusted developers would get users to authenticate through our endpoint then steal the patient's medical records through our API.**
   The applications that need to be allowed to access the APIs are selected by patients. App developers are not subject to HIPAA requirements, and payers are not allowed to refuse to share their information with the app the patients have chosen unless the app poses a security risk to the payer system. Payers have an obligation under the CMS final rule to educate members on these topics. CMS has provided materials to aid payers in educating their members.

2. **Is there a definition of clinical data?**
   Clinical data includes data elements listed in the US Core Data for Interoperability (USCDI) version 1 if maintained by the payer. In the final rule, CMS defines "maintain" to mean elements of the USCDI that the payer has access to, has control over, and has authority to make available through the API. CMS expects payer organizations to apply that definition in determining whether the rule applies to data in their systems.

3. **For members who are no longer enrolled in a plan, do you have to provide their data via the Patient Access API? How long do you have to provide that information? Is there a time frame for how far back the member was enrolled? 1 year, 2 years, or back to 2016?**
   The CMS final rule does not require payers to make data available through the Patient Access API after a patient is no longer a member. However, the payer must still make information available to the patient's new payer through Payer-to-Payer Exchange for 5-years after leaving a plan. It must include any data the payer has from January 1, 2016 onwards. If a patient has a gap in membership of longer than five years and then becomes a member again, the payer only has to provide data as far back as the end of that gap.

4. **What does "Payer Manages" mean, and does it differentiate received data (HIEs) from originally sourced data?**
   CMS finalized the rule with the verb "maintains" in place of the verb "manages". In the final rule, CMS defines "maintain" to mean that the payer has access to the data, has control over the data, and has authority to make the data available through the API. CMS has made it clear that payers are responsible for applying this definition to data in their systems. It is going to be important for payers to begin to look, now, at the language in the rule and to determine how they are going to interpret the language. That may mean getting legal and compliance departments involved to understand how to legally interpret the language. The definition of maintained data is an example where interpretation of the language will be required by each payer.

5. **Is there a requirement for payers to provide claims and clinical data to providers?**
   No. The CMS final rule is specific to APIs that allow patients to access their claims and clinical data. There is no requirement under the CMS Rule for payers to make information available to any individual other than patients.

6. **Is data not managed by the payer but aware of through HIE in scope within the USCDI?**
   No. The CMS final rule only requires payers to make claims and clinical data maintained by the payer available through the patient access APIs. Payers are under no obligation to retrieve additional data from providers or HIEs.

7. **Is there any addressing of an app developers' right to retain a copy of all the data collected, and what they might do with it? Or is that all addressed in whatever consent the patient gives when initiating the transfer?**
   App developers are not covered by the HIPAA Privacy Rule. They are subject to FTC regulations, and can do anything with the data that is allowed by FTC regulations. It is important for patients to understand that data available to them through their apps is not protected under HIPAA, and payers have an obligation under the CMS final rule to educate members on these topics. CMS has provided materials to aid payers in educating their members.

8. **It is not clear where the line is on data received in admin transactions versus managed data... what does it mean to manage data in the context of the rule?**
   CMS finalized the rule with the verb "maintains" in place of the verb "manages". In the final rule, CMS defines "maintain" to mean that the payer has access to the data, has control over the data, and has authority to make the data available through the API.

9. **How fresh must the data be? Can it be warehoused? 24 hours old?**
   Payers must make claims and clinical data available via the Patient Access API within 24 hours of receipt. There is very little information about how quickly a payer must retrieve the information and make it available on the API. However, API requests are generally responded to in near real time, so patient expectations are likely to be for an immediate response. CMS notes that the rule states that the specified data with a date of service on or after January 1, 2016 must be made available via the Patient Access API per the enrollee's request even if normally stored in archive, tape, or "cold" storage. That means payers should consider whether there is a need for data to be accessible in near real-time and not in "cold" storage that would require a long time to retrieve.

10. **Still seeking definition of "managed". We have clinical data we don't "go get" but is clinical.**
    CMS finalized the rule with the verb "maintains" in place of the verb "manages". In the final rule, CMS defines "manages" to mean that the payer has access to the data, has control over the data, and has authority to make the data available through the API. CMS has confirmed that payers are responsible for applying that definition in determining whether the rule applies to data in their systems, and notes that the rule does not limit the available data by how the data are being used.

11. **Assuming each dependent a member has would need their own login so that the API isn't returning records for the member plus their dependents with the same login. How should we handle when a member is no longer a dependent of the member who registered for them? Example the member turns 18 or cps is involved, and a parent should no longer have access to their child's medical records?**
    Payers are responsible for issuing login credentials to members that are then used to identify them to the API. Payers must ensure that information on (previous) dependents is not disclosed inappropriately. This may require payers to issue separate login credentials for dependents, or accurately managing dependent status. Payers also have an obligation under the CMS final rule to educate members on privacy issues concerning the Patient Access API which may include education on sharing login credentials with others.

12. **If we do not have member credentials for members now, does the five years start for members from the go live of this rule?**
    The Patient Access API requirement only applies to current members or new members after the compliance date. It does not apply to prior members. Plans do not need to respond to member requests for Payer-to-Payer exchange, even if they left the plan within 5 years of the compliance date.

13. **What rules are surrounding the 3rd party apps patients may choose? How does a patient know if the app developer or company are not "bad actors" and what is their security capabilities to prevent breaches?**
    App developers must conform with privacy requirements of the Federal Trade Commission (FTC). CMS is providing materials payers can use to educate patients about sharing their health information with third parties, and the role of federal partners like the Office for Civil Rights (OCR) and the FTC in protecting their rights.

14. **How do you determine the security of a patient's choice of app? Who is liable for a potential privacy/security issue?**
    The payer is not responsible for security of an app selected by the patient other than to properly authenticate the patient and authorize the app via the OAuth2 and OpenID Connect standards specified in the rule. FTC privacy requirements apply to the app developer. Payers must share data via the API with the app chosen by the patient unless it poses a security risk to the payer system.

15. **Does USCDI differ from CCDA and if so how?**
    Yes. USCDI, or the US Core Data for Interoperability, is a data content specification listing data elements and the terminology used for those elements to support interoperability. CCDA, or the Consolidated Clinical Document Architecture, is a data format standard for data exchange and is an example of how USCDI elements might be packaged for exchange. The FHIR standard required by the Patient Access API is a different way to also package USCDI data.

16. **I see HIEs don't qualify as an API. However, FHIR/HL7 messages and claims are shared there. Is there an option to utilizing an HIE to connect to members?**
    There may be a role for HIE in helping plans comply with requirements of the final rule. CMS allows a plan to choose a vendor, and if a HIE (1) has access to all of the required information, including claims and clinical data maintained by the payer, and (2) implements the required FHIR and OAuth/OpenID Connect standards and can authenticate and authorize the patient, a plan might be able to use an HIE to meet the obligations under the CMS rule.

17. **Patients bring a third-party app of their own choosing. How many apps should each plan expect to need?**
    It is not clear. There are about a dozen apps available today.

18. **When does this go into effect? 1/1/2021?**
    The compliance date for Patient Access and Provider Directory API requirements is January 1, 2021, but CMS will exercise enforcement discretion for this requirement until July 1, 2021.

19. **Might HIT Commons initiate/facilitate collaboration initiatives among CCOs?**
    That is an idea to explore.

CMS Interoperability and Patient Access Final Rule: Provider Directory API

21. **If the provider directory must be available for download, does that mean it can simply be a report the user can download from the app?**
    The provider directory must be available via an API that uses the FHIR standard and is accessible by an app of the patient's choosing. It cannot be posted as a .pdf or something similar and downloaded in the same format that you may be making that information available today.

22. **Is there a list of third-party applications available regarding patient access? Does the payer need to be registered with all apps in case a member decides to use any one of the apps or does the payer need to register after they are aware of a member wanting to use one of the apps?**
    We are not aware of any consolidated listing of potential patient apps at this time. There are at least a dozen different app developers that are making products available to patients today. The payer

must register any app a patient chooses. The rule requires payers to publish applicable technical requirements and attributes necessary for an application to be registered with any authorization server(s) deployed in conjunction with the API.

23. **What penalty(ies) will CCOs face if they fail to address these requirements by stated deadlines?**
    CMS has not provided detail concerning how these deadlines will be enforced and what penalties might be assessed.

24. **How will one know that the payer requesting data is authorized to request it (i.e. patient is now enrolled with them)?**
    CMS has established no technical standards for payer-to-payer exchange, including standards for communicating or asserting patient authorization for the request. This is an excellent opportunity for payers to collaborate.

25. **Will CCO's be able to utilize TOC data sharing that's currently set up between CCOs?**
    At this juncture there is not a definitive plan on the use of TOC data sharing to complete Payer-to-Payer obligations, or alternatively for Payer-to-Payer exchanges to meet TOC data sharing requirements. OHA needs to analyze how the Transition of Care rule overlaps with the payer to payer exchange requirements.

26. **Is Consent Management required from the get-go or has this requirement been deferred to a later date/phase in the final rule?**
    All of the transactions for Patient Access and Payer-to-Payer Exchange outlined in the CMS rule take place as a result of direct patient request. For such directed exchange, payers may be able to assume the patient has consented for the exchange they have requested. There are currently no requirements beyond those requested by the patient. CMS has established no technical standards for payer-to-payer exchange, including standards for communicating or asserting patient consent to share data in response to the request.

27. **How do you ensure security and privacy of the PHI?**
    CMS has established no technical standards for payer-to-payer exchange. However, HIPAA Privacy and Security Rules apply. Absent future guidance form CMS regarding technical standards, payers must establish secure means to exchange information that protects PHI.

28. **With regard to consent management, when a member expresses an interest in exchanging data with an app, don't they need to consent to the specific type of data to be exchanged with each app?**
    Some app developers may allow patients to request only a subset of their data via the Patient Access API. FHIR can be used for granular access to data - e.g., only to request and receive a list of medications but not a list of problems or procedures or other clinical information. That requirement falls to the app developer.