OHA Federal Interoperability Final Rule Webinars: FAQ

This document captures the questions raised in the 10/1/20 HITOC-sponsored Federal Interoperability Final Rules Webinar and the 11/5/20 CCO/Payer Federal Interoperability Final Rules Webinar. The FAQ 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 ONC and CMS 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.

10/1 HITOC-sponsored Federal Interoperability Final Rules Webinar materials:

- Slides
- Handout
- Webinar recording

11/5 CCO/Payer Federal Interoperability Final Rules 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

Links to final rules:

- ONC 21st Century Cures Act Final Rule
- CMS Interoperability and Patient Access Final Rule

OHA Interoperability Final Rules Contact:
Please contact Marta Makarushka at Marta.M.Makarushka@dhsoha.state.or.us with questions.

Webinar Questions & Answers

ONC Cures Act Final Rule: Policy 1 Updates to EHR Certification Criteria

1. **If an app developer spills data we provide them, are we responsible for breaches?**
   A provider that makes health information available to patients at their request, in the method that they are requesting, is not responsible for a breach if that information is further disclosed after that lawful disclosure. App developers may not be subject to HIPAA privacy rules, so information disclosed by an app developer may not be a HIPPA violation or qualify as a breach. The question to keep in mind is whether patients know their app developer may not be covered by HIPAA privacy protections, and that app developers can use that information in any way allowable under Federal Trade Commission (FTC) rules, not HIPAA rules. While not the responsibility of the disclosing provider, patients should be made aware that their app developer is not prohibited from using the health information they obtain, for instance, for targeted marketing.

2. **Does the API rule require reading and writing through FHIR to the EHR or just being able to read and not write from the EHR?**
   Both the patient access rule in certification criteria and the patient access rule in the CMS rule for payers are for read access only. They are for the sole purpose of making clinical data (and, for the CMS rule, also claims data) available to the patient. There is no requirement that FHIR be used to send data to the EHR or the payer system.

ONC Cures Act Final Rule: Policy 2 Exceptions to Information Blocking

3. **Is there a delay in the information blocking penalty, do we know when that is?**
Yes and no. On 10/29/20 ONC published an extension to the compliance date until April 5, 2021. OIG has proposed that it would not enforce information blocking further until 60 days after publication of its final rule on enforcement and penalties for information blocking. Information blocking will not be enforced before April 5, 2021, we don't know when it will be enforced because OIG has not put out its final rule yet.

4. **Are we responsible for data where we are not the source of truth (e.g., medications)? Are we expected to provide health information we have access to?**
Yes, providers must pass on all clinical data that is included in the United Stated Core Data for Interoperability (USCDI). Data provenance, a new requirement under the USCDI, allows providers to identify who is responsible for generating that data so that the recipient will know the source and can determine the trustworthiness of the information. Yes, providers are required to share all of the information in the USCDI (which includes a medication list) independent of provenance (original data source).

5. **Are CCOs considered HINs w/regard to information blocking?**
ONC created a functional definition for HINs. However, whether a CCO is an HIN is not a question ONC can or will answer. ONC instead has said that the answer is not about the characteristics of an organization, it is instead about the functions they undertake. The definition of a HIN published by ONC includes any entity that determines, controls or has the discretion to administer any requirement, policy or agreement that permits, enables or requires the use of any technology or services for access, exchange or use of electronic PHI among more than two unaffiliated individuals or entities that are enabled to exchange with each other for a treatment, payment, or healthcare operations purpose. CCOs should look at that definition and the functions they control or facilitate in exchanging information and determine whether it applies to them. ONC is unlikely to rule on whether CCOs are HINs. In the CCO contract we have noted that CCOs need to determine that for themselves.

6. **Do the rules include eReferral exchange?**
eReferrals are not part of the USCDI at this time so, no, eReferrals fall outside of the requirements for the data that must be shared for patient access in both the CMS and the ONC rules, and outside of the data that must be shared to avoid information blocking. Note however that consultation notes must be shared.

7. **Does information need to be made available for immediate release to not be considered information blocking? For example, a 3-day delay on labs?**
The answer really depends upon the reason that the information is not immediately available. The Privacy Exception might provide reasons for delays to get patient consent. The Security or Health IT Performance exceptions might provide reasons for delays due for IT infrastructure issues. ONC has stated that timely access to data must be provided, but has not established a set timeframe for what “timely” access means because there is so much variability regarding what “timely” will mean given the broad scope of health IT involved. ONC instead emphasizes that whether access is considered timely will be determined based on the specific facts and circumstances.

   The CMS final rule requires payers to provide patients with access to clinical data with 24 hours of receipt.

8. **Are Community Information Exchanges (CIEs), such as Aunt Bertha and Unite Us, included in these rules?**
   To extent that the community information exchange performs actions that meet the definition of a Health Information Network (HIN), answer is probably yes. The definition of HIN includes any entity that determines, controls or has the discretion to administer any requirement, policy or agreement that permits, enables or requires the use of any technology or services for access, exchange or use of electronic PHI among more than two unaffiliated individuals or entities that are enabled to exchange with each other for a treatment, payment, or healthcare operations purpose. If the CIE is only exchanging health or community services information for reasons other than treatment, payment, or health care operations, such as to meet housing needs, food support needs, etc., it may not be a HIN because the exchange is not for treatment purposes. You can't say yes or no whether any CIE in general does or does not meet definition of a HIN, as the definition is functional, not based on specific organization characteristics.

9. **Is there anything that limits the fees EHR vendors can charge providers to exchange data? And if not, if an EHR vendor charges a rate that is much higher than others can that be determined to be information blocking?**
   Yes, unreasonable fees associated with interoperability might constitute information blocking. Organizations are allowed to charge fees, or to license their software for purposes of exchanging information. The Fees and Licensing exceptions list limitations on what those fees may be. They may not be excessive and they must be traceable to actual effort required to provide that service.

10. **What state specific laws are on your radar as relates to information blocking rules?**
    Disclosures required by CMS (and ONC) rules are subject to state restrictions, such as regulation on the disclosure of BH information, HIV status, minors, etc.

11. **Do these rules apply to data held by the state?**
    Certification and information blocking provisions apply to a state only under certain circumstances. Information blocking applies to the state if the state meets the criteria of a health information network (HIN) as defined in the ONC final rule.

CMS Interoperability and Patient Access Rule: Patient Access and Provider Directory APIs

12. **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.

13. **Is the state under the same requirement as the CCOs?**
    The requirement to provide Patient Access and Provider Directory APIs extends to Medicaid and CHIP fee-for-service programs (as well as to other CMS-regulated payers).

14. **When do the API requirements go into effect?**
    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.

15. **Will OHA be providing a patient portal?**
    There is no requirement in the CMS rule for a payer to provide a patient portal. The requirement is to provide an access API (a program interface) that the patient can use with the third-party app (e.g., an app on their smart

phone) to download their data and provider directory. The requirement to provide patient access and provider directory APIs extends to Medicaid and CHIP fee-for-service programs (as well as to other CMS-regulated payers).

16. **What solutions/vendors will OHA fee-for-service employ to achieve API compliance?**
OHA will make this information available once they have completed the special procurement process.

Interoperability and Patient Access Rule: Patient Access API

17. **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. Access 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.

18. **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.

19. **If an app developer spills data we provide them, are we responsible for breaches?**
A payer that makes health information available to patients at their request, via the method requested, is not responsible for a breach if that information is further disclosed after that lawful disclosure. App developers may not be subject to HIPAA privacy rules, so information disclosed by an app developer may not be a HIPPA violation or qualify as a breach. The question to keep in mind is whether patients know their app developer may not be covered by HIPAA privacy protections, and that app developers can use that information in any way allowable under FTC rules, not HIPAA rules. The disclosing payer is required to make patients aware that their app developer is not prohibited from using the health information they obtain, for instance, for targeted marketing.

20. **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.

21. **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 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.

22. **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.

23. **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.

24. **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.

25. **For the Patient Access API, what is the mechanism of authenticating members?**
Access to health information through the patient API must use the SMART Application Launch Framework Implementation Guide Release 1.0.0, which specifies how OAuth2 and OpenID Connect are used to authenticate a patient and authorize the third-party app’s access to health information. EHR portal access for patients has been a requirement for some time, so there is probably a mechanism most providers have put in place to create and manage login IDs and passwords for patients that can support patient access using SMART. Payers may need to develop processes to create and manage patient credentials.

26. **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.

27. **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.

28. **What is the definition of an administrative transaction as used for these items?**
Plans get health and health-related information through what are sometimes called "administrative transactions" or HIPAA transactions or X12 transactions that have certain data dictionaries associated with them and a certain organization that differs significantly from what the FHIR standard is requiring. Plans will need to translate from the format and terminologies used to currently get that type of information into a new data model defined in FHIR. That process and those mappings may be foreign to their vendors and something they need to plan for.

29. **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.

30. **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.

31. **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.

32. **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.

33. **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

34. 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.

35. 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.

36. 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.

37. Is translation of information required if a patient doesn't speak English?

The CMS final rule does not specify requiring translation.

38. Does the API rule require reading and writing through FHIR to the EHR or just being able to read and not write from the EHR?

Both the patient access rule in certification criteria and the patient access rule in the CMS rule for payers are for read access only. They are for the sole purpose of making claims and clinical data available to the patient. There is no requirement that FHIR be used to send data to the EHR or the payer system.

39. Is there a requirement for payers to provide claims and clinical data to providers?

The CMS Interoperability and Patient Access final rule is specific to APIs that allow patients to access their claims and clinical data. There is no requirement under this CMS Rule for payers to make information available to any individual other than patients. The CMS Reducing Provider and Patient Burden proposed rule adds a proposed requirement for payers to build and maintain a Provider Access API for payer-to-provider data sharing of claims and encounter data (not including cost data), clinical data as defined in the U.S. Core Data for Interoperability (USCDI) version 1, and pending and active prior authorization decisions for both individual patient requests and groups of patients starting January 1, 2023.

40. What, if any, work should individual healthcare systems expect as a result of the new payer requirement under the CMS Interoperability and patient access final rule?

Nothing associated with patient access or payer to payer exchange in the CMS rule applies to healthcare systems.

41. **If a *clinic* has claims in their data warehouse is it incumbent upon them to share the claims, or are those the responsibility of the plans?**
    The CMS rule doesn't apply to health systems or providers. What is required for patient access for providers are the USCDI data elements, and only the USCDI data elements. Claims are not included in the USCDI data elements. If providers do have claims in their system, they don't need to provide them, and yes the patient can get claims from their plan instead.

42. **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.

Interoperability and Patient Access Rule: Provider Directory API

43. **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.

CMS Interoperability and Patient Access Rule: Payer-to-Payer Exchange

44. **For payer-to-payer exchange are there any candidate API standards recommended by OHA or CMS that are likely to be adopted nationally; that is, is there a coordination effort in progress?**
    Not from within the CMS Interoperability and Patient Access final rule. The CMS Reducing Provider and Patient Burden proposed rule specifies implementation guides for this API.

45. **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.

46. **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. The CMS Reducing Provider and Patient Burden proposed rule specifies implementation standards for communicating and asserting patient authorization.

47. **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.

48. **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 Payer-to-Payer Exchange and Patient Access API 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.

49. **Does OHA intend to play a role in establishing/proposing a technical standard for payer-to-payer data exchange applicable to CCOs?**
OHA will not have a mandate. However, the CMS Reducing Provider and Patient Burden proposed rule specifies implementation guides for this API

50. **How does the plan provide USCDI data when it is not collected?**
The CMS rule only requires a plan to exchange USCDI data elements that are maintained by the payer. It does not require the payer to obtain additional USCDI data elements not maintained by it from the providers rendering care.

51. **How do payers exchange USCDI data when they don't manage it and it's in the patient's EHR?**
The CMS rule requires payers to exchange claims data and clinical data maintained by it, if the clinical data is in the USCDI. If a payer doesn't maintain that data already, it is not required to obtain that data from the providers and provide it to patients. Payers are only required to provide access to clinical data that is already maintained by it and that they obtained through existing processes.

52. **Do these rules apply to data held by the state?**
CMS-regulated entities, including state Medicaid and CHIP programs, must provide patient access to their claims and clinical information based on the CMS final rule provisions.

Interoperability and Patient Access Rule: Provider Requirements

53. **Since CCOs as payers cannot apply for an NPI with NPPES, do the last three CMS requirements apply to CCOs?**
The requirement for listing your digital contact information is a provider requirement, not a payer requirement, even though it appears in the CMS rule. The last 3 areas in the CMS rule, the attestation that you're not information blocking, the requirement to list digital contact info in NPPES, and the ADT event notification requirement are provider requirements and not payer (or CCO) requirements.