Ready for Submission

1. Do payers need to support requests for all data on an enrolled member in a covered plan at any time in the Patient Access API or can we only make new data available once the application has requested and received all data back to 1/1/2016?

   The rule does not limit a payer’s obligation to a delta file of new data.

2. If information is exchanged from a prior payer to the current payer at member direction, and the information is not in the Patient Access API format, it is our understanding that the current payer does not need to make this information available via the Patient Access API. Is this correct and is this not considered data blocking?

   Per the final rule, data received via the payer-to-payer data exchange only need to be made available to share in the electronic form and format they were received from another payer (see 85 FR 25567). As a result, if a payer receives data from a current enrollee’s former payer via a FHIR-based API under this payer-to-payer data exchange provision, and then the enrollee asks that their data be made available via the Patient Access API, the previous payer’s data should be included in the data made available via the Patient Access API. It is not information blocking to only make available those data specified in the regulation as available via the API. However, all existing federal, state, and local laws apply, and if the patient requests their record outside of the Patient Access API, then a payer must accommodate existing law governing the patient’s request.

3. If information is exchanged from a prior payer to the current payer at member direction, and the information is in the format used by the Patient Access API, is the current payer required to make this prior payer’s data for the member available via the Patient Access API? If it is optional and the current payer elects to not include the information in the Patient Access API is this considered data blocking?

   If a payer receives data from a current enrollee’s former payer via a FHIR-based API under the payer-to-payer data exchange provision, and then the enrollee asks that their data be made available via the Patient Access API, the previous payer’s data should be included in the data made available via the Patient Access API (see 85 FR 25567). As these data would need to be shared, there are no implications for information blocking.

4. If a payer has the same information available from multiple sources (claims, CCD, ORU) for the same event (e.g. procedure) or for the same element from multiple events (e.g. diagnosis) and the payer makes the information available once for each occurrence does that meet the requirements of the rule?
All claims data with a date of service on or after January 1, 2016 must be made available via the Patient Access API. For data elements included in the USCDI version 1, payers must make available those data they maintain with a date of service on or after January 1, 2016, as well. If the same data element is included in the enrollee’s record from multiple sources for the same event, that information only needs to be mapped to FHIR and made available via the Patient Access API once. This would ensure this single event is represented, but duplicate information for that single event is not included. As other data elements may remain constant for some time and/or change over time, payers should look at the data they maintain and ensure that information relevant to the patient’s care and treatment over time is accurately represented – in this way, it may not be appropriate to include a single data element only once across multiple events.

5. If an EHR charges to “register” an application used by a payer to obtain information required for permitted purposes (e.g. payment, operations, care coordination), does this constitute information blocking? (currently certain EHR vendors charge over $20,000 and an annual maintenance or usage fees)

For questions related to vendors and information blocking, contact ONC via the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

6. Are there required metrics for information security (e.g., levels of denial of service attacks, number of inquiries per unit time, etc.) that plans can employ to appropriately revoke access to third parties and avoid risk of information blocking violations?

Per the final rule, payers may only deny or discontinue any third-party application’s connection to their API if the payer reasonably determines, consistent with its security analysis under 45 CFR part 164 subpart C, 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 or in transit in instances in which the individual did not tell the payer to disregard in-transit risk. When access has been denied or discontinued due to security concerns, we encourage payers and third parties to work together to address the concerns if and as possible to best serve patients. We are not able to set a specific time period or process for this as it is beyond our authority, however, we do note that the HIPAA Privacy Rule requires access to be provided to the individual in a timely manner (see 85 FR 25548).

The criteria and process for assessing unacceptable risk to a payer’s system are part of the payer’s responsibilities under the HIPAA Security Rule. The HIPAA Security Rule requires a covered entity to perform risk analysis as part of its security management processes (45 CFR 164.308(a)(1)(ii)(A)). HHS makes a number of tools available to assess risk (For more information, see https://www.hhs.gov/hipaa/for-professionals/security/index.html). Additional tools are available through the National Institute of Standards and Technology (NIST) (see https://csrc.nist.gov/publications/detail/nistir/8062/final).

7. What is the definition of “processing” claims and encounter data to be made available “no later than one business day” in the patient access API? Does the period start on:

7.1. receipt of the claim by payer or contracted claims processor
7.2. after adjudication (partial or full)
7.3. Is the answer impacted if the payer only processes claims periodically (e.g. once a week)?

We finalized that payers make available through the Patient Access API, no later than one (1) business day after the information is received: (1) adjudicated claims, including claims data for payment decisions that may be appealed, were appealed, or are in the process of appeal, and (2) encounter data. We reiterate that this is one (1) business day after the claim is adjudicated or encounter data are received. This allows for potential delays in adjudication or delays in providers submitting their encounter data. It does not require payers and providers to change their contractual relationships or current processes for receipt, though we strongly encourage payers and providers to work together to make patient data available in as timely a manner as possible (see 85 FR 25535).

8. What is the definition of next business day? If information is received between 12:01 AM and 11:59 PM on a business day does "the next business day" end at 11:59 PM the next business day (all times assumed local to site where processing occurs)?

Generally, CMS considers receipt by close of business (generally between 4 and 5pm) to be within the business day. After close of business, would not be considered receipt until the start of the next business day. Therefore, if a claim is adjudicated and available to the payer to share starting at 6pm on a Monday. The one business day clock would not start until Tuesday start of business. And, the claim would not have to be made available to the patient until Wednesday, the earliest.

9. Although the payer’s provider directory API may not require a member account for secure access, is service level security permissible with the provider directory API?

9.1. Can payers enforce service level security (to prevent denial of service attacks, exposure to bad actors, SQL injection, etc.)?

9.2. Is there any restriction on putting basic best practices in place to make the Provider Directory API accessible and prevent attacks on its availability?

The Provider Directory API endpoint must be made publicly accessible. Specifically, the rule requires payers make the Provider Directory API accessible via a public-facing digital endpoint on their website to ensure public discovery and access. Payers must exclude the security protocols related to user authentication and authorization (required for the Patient Access API) and any other protocols that restrict the availability of this information to anyone wishing to access it. As this is not PHI, and generally publicly available information at this time, restrictions are not permitted (see 85 FR 25560 through 25564).

You can put this information behind an initial firewall in order to protect against things like a denial of service attack, much as you would currently protect data available via your website, but otherwise this must be a truly public and unrestricted digital endpoint.

10. Does data collected by payers for risk adjustment, quality improvement, or utilization management that is also considered part of USCDI, e.g., conditions/diagnoses, need to be shared as part of USCDI via the Patient Access API? Or only is it was obtained through clinical data sources such as CDA documents and ORU result messages?
All USCDI data that the payers maintain as part of the enrollee’s record are to be made available via the Patient Access API. 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 (85 FR 25538). The rule does not limit the available data by how the data are being used or the purpose for which they were originally received. If the data are currently maintained, they must be made available via the Patient Access API.

11. If a payer uses a partner to administer specific benefits (e.g. drug benefit) and the partner collects clinical information as part of the normal process (e.g. allergy intolerances gathered from patients before dispensing medications), is this data in the scope of clinical data maintained by a payer and must be made accessible through the Patient access API?

This goes back to the definition of ‘‘maintain’’. It is up to each payer to assess your relationship with the partner to understand if these data would be within your access, control, and authority to share. A contracted relationship where a partner is collecting and maintaining data on behalf of the payer would generally qualify as data “maintained” by the payer.

12. If a covered payer requires an application that wishes to access the Patient Access API to meet specific industry standard requirements for secure access to confidential information in addition to compliance with OAuth 2.0 and OpenID Connect to ensure that an application will not present a risk to the payer systems, does this violate the CMS final rule?

Additional security, such as the use of multifactor authentication, for instance, is supported by the required standards. SMART on FHIR, and specifically the OAuth 2.0 standard HHS has finalized provides robust support for multifactor authentication. Such additional security is not prohibited via the technology or the specifications in the rule. As noted in the final rule, by requiring that payers subject to our Patient Access API requirement use an API that is conformant with 45 CFR 170.215, where HHS has finalized the SMART IG, we are supporting the use of multifactor authentication (85 FR 25545).

13. Payers require, from a security and audit perspective, that the authorized third-party application must use the OAuth token issued by the payer for a specific individual that has been granted access to the information. This token cannot be used by the application to allow another individual to “act on behalf of the member”. By this we mean that access by an “authorized representatives” cannot be granted the ability to use another individual’s (e.g. the member’s) token. The payers will enforce the requirement that the token is issued and may only be used for a single application and individual context. This would be considered a security violation and the basis for denying the application’s access to the API. Does this violate any portion of the CMS final rule regarding access to the Patient Access API.

We note that OAuth is a delegation protocol to act on the patient’s behalf. And, we note that per the final rule, when we discuss patients, we acknowledge a patient’s personal representative. According to the HIPAA privacy regulations at 45 CFR 164.502(g), a personal representative is someone authorized under state or other applicable law to act on behalf of the individual in making health care related decisions (such as a parent, guardian, or person with a medical power of attorney). See OCR guidance regarding personal representatives at
Policies in this final rule that require a patient’s action could be addressed by a patient’s personal representative (see 85 FR 25514). In this way, a token would have to be granted to the patient’s personal representative on the patient’s behalf, just as the payer would have to provide access to a patient’s health information to their personal representative if requested on the patient’s behalf today.

14. We assume that the payer’s API and supporting consent model govern right of access and issue a specific credential (such as a token) for each beneficiary and authorized individual as opposed to the application handing such credential management?

The expectation is that the payer will maintain a protected resource server, which will be looking for a token from the app to provide the role and access rights of the enrollee. If the token is not valid, the protected resource server should direct the enrollee request to the authorization server. The authorization server can establish the identity of the enrollee either itself or by interacting with a separate identity server. Either way, a screen (or series of screens, if necessary) can be displayed where the patient provides the necessary credentials (such as user name and password, multi-factor authentication, retina scan, etc.) to establish their identity. For the best enrollee experience, this would ideally be done within the client web or mobile app itself and not require the enrollee to manually visit another portal themselves.

When the authorization server is satisfied with the identity and access request, an access token is generated representing the role and access rights for the enrollee, which can be used by the app on subsequent requests to the protected resource server. A separate identity token can also be generated to allow systems to get more information about the identity of the enrollee, if needed (e.g. address, phone number, etc.).

The authorization server is an integral part of the API. When the request arrives at the API from the third-party app, if there is a token, and it is valid, then the data exchange is authorized. If the token is not valid -- for instance if it is expired or not for the specific information being requested, etc. -- an authorization error will be returned. This is all part of the API, done through a series of forwarding requests.

15. Confirm that within the context of the rule, a representative is not distinguished or managed based upon their relationship with the beneficiary and are all handled the same? An example would be that a representative may be a spouse or may be PCP, but for the purposes of representation, the payer doesn’t change API behavior based upon the relationship. A representative is a representative and is treated the same regardless of the relationship between the representative and the beneficiary OR the relationship between the representative and the payer (other than for issuance of the token).

Please see the response to question #13 above. For the Patient Access API, the request would have to be initiated by the patient or their personal representative.

16. There is a substantial difference in the implementation effort and risk (e.g. errors, completeness, clinical context) of taking unstructured data (e.g., PDF, jpeg, or other unstructured formats) and converting the USCDI data elements contained in it to FHIR resources versus using the FHIR
DocumentReference resource to make the unstructured data available via the Patient Access API. Operational concerns of payers include the following:

   a. Non-standard, inconsistent conversion of unstructured data to FHIR by each payer creates risk in the interpretation of the information
   b. The NLP method of conversion of unstructured data will differ by vendor, and results in variability of the FHIR content
   c. The Provenance of the FHIR output in Payer-to-Payer, to document that the source was a PDF conversion will be a challenge to the receiving payer if the sending payer does not accurately and consistently document and identify the source as originally a PDF.

Covered payers need immediate guidance from CMS indicating if using DocumentReference to exchange unstructured data meets the requirements of the final rule with regard to clinical data received by the payer as unstructured data.

Regarding unstructured data such as a large PDF or a scan of a fax that may or may not include data elements in the USCDI, we note that payers should focus on the USCDI data that can be identified at the data element level – data that a payer maintains as part of an enrollee’s record as a discrete data element that the payer can then map to FHIR and make available via the Patient Access API. We strongly encourage payers to work to make as much data available to patients via the Patient Access API as possible to ensure patients have access to their data in a way that will be most valuable and meaningful to them, but we are not asking payers to manually go through large files that cannot be parsed into data elements efficiently for the purposes of this API. And, we are not asking payers to include these large files in the data available via the API.

17. While the directory data for a covered payer is required to be openly available, the formulary data for the same covered payers (where applicable) is required to be part of the Patient Access API. If formulary is included as part of the Patient Access API, it will be subject to the same authentication and authorization process as the remainder of the members claims and clinical data. The implementation guide cited on the CMS web site (PDex Formulary) does not provide for plan member authentication and authorization.

   a. Is the requirement to present formulary information only in the context of the member?

   b. If so, this information will not be available for consumers to compare drug coverage by different drug benefit plans. Is this the intent of the final rule?

   c. If not, please provide clarity on the expectation for access to formulary?

   d. If a covered payer chooses to make the formulary only openly available (e.g. not part of the Patient Access API) is this considered compliant with the final rule?

The rule does not prohibit making formulary data openly available, just like the Provider Directory data. There is no prohibition in the rule to making the formulary endpoint publicly accessible. This would support implementing the “Shopping for Health Plans” use case detailed in this implementation guide (IG). Supporting this use case is not required by the rule, but it not prohibited.
The final rule does require that the formulary data specific to the patient in question be made available via the Patient Access API. As such, access to the formulary service when integrated with protected health information (PHI) or personally identifiable information (PII) as part of the Patient Access API shall be protected through an authorized, authenticated transaction. Additional information about this use case has been added to the PDex Formulary IG.

18. If a member directs a plan to share information with another plan and the member chooses to do so in such a manner that the same information is provided by more than one prior plan (e.g. Plan B has Plan A’s information from a prior request to share and the member directs both A and B to share the information with plan C),
   
   a. Is it the responsibility of each plan to indicate if the information comes from a prior plan?
   
   b. Is it the responsibility of the receiving plan (e.g. Plan C) to identify and eliminate duplicate data?
   
   c. If the information is in Patient Access API format, is it acceptable to present all of the received data (from both Payer A and Payer B) via the Patient Access API with any duplication of data included?

If a payer gets a request from a member to share data with another payer, the payer’s only obligation is to make the required data available to the designated payer. Payers have the ability to indicate the provenance of the information they are sending. Receiving plans are not required to deduplicate data they have received from other payers. If a payer receives information under the payer-to-payer data exchange via an API, and subsequently shares those data via the Patient Access API, the payer is again only obligated to send the required data they maintain. They are not required to deduplicate or otherwise review or validate data they receive from another payer.

19. With respect to the term adjudication in final rule, is it CMS’s intent that this process is complete (e.g. starts the 1 business day clock) when the claim processing is finished or when the provider payment process is completed. There may be several days of delay between the processing of a claim and the payment to the provider, during which the provider may question the reimbursement and adjustments may be made that need to be reflected in the EOB.

   a. Does the 1 business day clock start on completion of claims processing or on completion of initial payment to the provider?

By “adjudication,” we mean determination of whether a given claim is entitled to reimbursement pursuant to the terms and conditions of a particular plan, and the amount payable to and by relevant parties. We appreciate that adjudication is a process, however. Because it is a process, and that process varies by payer, adjudication is not defined as always pre- or post- payment. Ultimately, a payer needs to assess their system and their process, and in good faith work to get patients information timely. If edits were still pending on a claim even if the claim was in approved status, for instance, one could argue that claim is not fully adjudicated as the impending edits could change the amount to be paid by whom based on the given payer’s process.
20. How long does a covered payer have to register a third-party application so that a member may use the application to access the Patient Access API?

The rule does not specify a time period, but we do point to the ONC 21st Century Cures Act final rule for guidance on this. In alignment with requirements in this rule, we suggest tokens be valid for at least 3 months (see 85 FR 25746).

21. During the September HL7 Connectathon several questions were raised regarding the open access to a covered payer’s provider directory. We acknowledge and support the goal of not requiring additional actions/steps by the consumer/member in accessing the provider directory information. However, several questions were raised regarding open access and application registration:

a. If a covered plan publishes their provider directory as a PlanNet compliant collection of resources (e.g. as a bundle or in ndjson format) on an openly accessible site, would an API supporting retrieval of such files (e.g., GET /path/to/directory.ndjson) satisfy CMS requirements for open access?

b. From an API security and performance perspective, all API consumers (apps, not users) should be known and use an API key (or other auth mechanism) so the covered knows the identity of the applications/developers (this is standard industry approach today). Several mechanisms are widely and commonly used by organizations offering public access APIs; for example using a public anonymous token, or a clientID/Secret combination. This approach would not make it any harder for an individual to use the API, nor require individuals to identify themselves. However, it will ensure the service can properly track the application being used and protects the API from attacks (which would now be traceable to the registered application). Are these practices within scope of the rule to provide API access to covered data?

The final rule requires payers make the Provider Directory API accessible via a public-facing digital endpoint on their website to ensure public discovery and access. Payers must exclude the security protocols related to user authentication and authorization (required for the Patient Access API) and any other protocols that restrict the availability of this information to anyone wishing to access it. As this is not PHI, and currently publicly available information, restrictions were not included.

You can put this information behind an initial firewall in order to protect against things like a denial of service attack, much as you would currently protect data available via your website, but otherwise this must be a truly public and unrestricted digital endpoint.

We strongly suggest the use of the PlanNet IG to meet this requirement. And, in August, through the Medicaid State Directors letter, the use of the PlanNet IG was required for state Medicaid agencies seeking to access the enhanced FFP (see https://www.medicaid.gov/federal-policy-guidance/downloads/sho20003.pdf).
22. Can EHR vendors prevent payers from using a SMART on FHIR app appropriately registered with an EHR vendor for a permitted purpose?

The CMS Interoperability and Patient Access final rule does not regulate EHR vendors. For additional information about requirements for EHR vendors, we suggest reviewing the ONC 21st Century Cures Act final rule. More information is available here: https://www.healthit.gov/curesrule/.

Additional information on Dental and Vision claims:

We do note that although the rule does not exclude vision and dental claims, we appreciate that the CARIN IG for Blue Button cannot currently support dental and vision claims data. This is the IG we suggest that payers use to make claims data available via the Patient Access API. Generally, if a payer uses the suggested IGs and follows the IGs to spec to build their API, from a technical perspective, the payer will be in compliance with the final rule. As a result, until dental and vision claims are supported by the CARIN IG for Blue Button, we understand that they will not be available via the Patient Access API.

**** DISCLAIMER ****

These responses were current at the time they were provided by CMS. This document was prepared as a service to the public and not intended to grant rights or impose obligations. This document may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be general information. It is not intended to take the place of either written law or regulations. We encourage readers to review the specific statutes and regulations for a full and accurate statement of their contents. Please feel free to share this information with your constituent members, organizations, or interested parties.

Individuals may send additional questions to the CMS Health Informatics and Interoperability Group (HIIG) at CMS_HealthInformaticsOffice@cms.hhs.gov.