Da Vinci is seeking answers to open questions and clarifications needed on the upcoming CMS Patient Directed API Rules. Find questions discussed by the Da Vinci Payer group and disposition including whether question was answered by CMS. The pdf format responses are here: Set 1, Set 2, Set 3, Set 4, Set 5, Set 6 (Note: questions in set 7 were combined into set 6 as questions 12-15.), investigating set 8 status and existence, Set 9

CMS included the following statement with responses received:

These responses have been provided by the Health Informatics and Interoperability Group at CMS and are based on the Interoperability and Patient Access final rule (CMS-9115-F) published on May 1, 2020. The responses reflect current information from the final rule and do not constitute new policies nor create new requirements on the public. Please feel free to share this information with other individuals and organizations to whom it may apply.

**** CMS DISCLAIMER ****

These responses were current at the time they were sent. 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 the 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.

### CMS Final Rule Questions and Answers log

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Category Keywords</th>
<th>Question</th>
<th>Date Received</th>
<th>Disposition / Answer</th>
<th>Date Resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Provenance</td>
<td>1) The definition of provenance in USCDI requires both the data/time at which the information was created as well as the organization associated with the individual that ‘used’ the data. Payers frequently will not have knowledge of the actual date/time of creation of the specific organization that created the data (they know the organization from which it was received): May the payer provide a non US Core profile on the provenance resource (as specified by the Da Vinci PDex IG) to indicate that the payer is the transmitter and optionally, a second provenance resource to indicate the source of the information and method of receipt (e.g. received from xxxxxxx organization on x via a CCDA)? If not, should the payer make a US Core provenance resource available and use a data absent reason for unknown data, or b. exclude the provenance resource?</td>
<td>23-Jun-2020</td>
<td>Response: Appreciating the additional value the PDex IG provides for payers, and the compatibility of the PDex IG with the US Core IG, we are adding PDex as ‘suggested’ option available to payers to meet the requirements of the rule. This information is being added to the CMS website: <a href="https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index">https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index</a></td>
<td>13-Jul-2020</td>
</tr>
<tr>
<td>1002</td>
<td></td>
<td>2) Please clarify the Payers obligation to make data (e.g. claims, encounter, clinical) available via the member access API in the following situations: a. Payer uses separate legal entities to provide different covered plans (e.g. Medicare Advantage and Medicaid HMO). Is the payer required to make the data from all plans available to the current enrollee in one of the plans via the member API? If yes, are multiple APIs acceptable? b. If the current enrollee in a covered plan (e.g. Medicare Advantage) was previously enrolled in the same or another covered plan (e.g. QHP in Federal Marketplace) is the payer required to make the data available from all covered plans via the member API? c. Is the payer required to make data available from a non-covered plan (e.g. commercial coverage and not a qualified QHP) when the member is enrolled in a current covered plan (e.g. Medicare Advantage)? d. If a member leaves the payer for five years and then returns as an enrollee in a covered plan (e.g. Medicare Advantage) is the payer required to make data available to the member via the member API going back to 1/1/2016? e. Must enrollees have access to all prior coverage to the third-party app or can they restrict the data to only the current covered plan? f. If the payer is not required to make the data from a prior enrollment (regardless of plan type) available in the member API, is the payer required to make the data available via the Payer to Payor requirement as of 1/1/2022?</td>
<td>23-Jun-2020</td>
<td>Response: (a) If the patient is a current enrollee in the Medicare Advantage plan, the payer is required to make all data they maintain for that patient as part of their enrollee record within the Medicare Advantage plan. Critical here is the definition of ‘maintain’. 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). If the data meet this definition of maintain per the payer’s assessment and are part of an enrollee’s record, the data would need to be made available via the Patient Access API upon the patient’s request. If these maintained data are not currently in a FHIR format, these data would need to be converted to a FHIR format and shared via the Patient Access API. How a payer chooses to implement the API (one or many), is completely up to the payer. b. Response: As noted above, this goes back to how the payer “maintains” the data for the enrollee in their current plan. No, this is not required. Again, this goes back to how the payer “maintains” the data. c. Response: No, this is not required. Again, this goes back to how the payer “maintains” the data. d. Response: All payers need to make data they maintain for their current enrollee with a data service on or after 1/1/2016 available. If an enrollee is with a plan from 1/1/2016 through 1/1/2021, leaves, and returns 1/1/2026 it would depend on how the payer maintains the data from 1/1/2016 through 1/1/2021. If these data are maintained and part of the enrollee’s record upon their return in 2026, then, yes. If the payer essentially considers the enrollee a new member in 1/1/2026 and has not maintained the previous year’s data as part of the enrollee’s record, it would not be part of the enrollee’s record and would not be available via the Patient Access API. We note that all existing and applicable data retention requirements are assumed to be taken into account here by the payer, as appropriate. e. Response: Starting in July 2021 when compliance with the Patient Access API is officially enforced, all specified data the payer maintains for the enrollee with a data service on or after 1/1/2016 must be made available. If the payer maintains data other than data from the current covered plan as part of the enrollee’s record, then it would be included in what is available. Again, this goes back to how the data are maintained. f. Response: As with the Patient Access API, the Payer-to-Payer data exchange is based on the USCDI data the payer maintains as part of the enrollee’s record. That said, 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 their data be made available via the Patient Access API, the previous payer’s data should be included.</td>
<td>13-Jul-2020</td>
</tr>
</tbody>
</table>
3) With respect to information received via a claim or encounter: a. Is there any prohibition against including relevant data classes (e.g., procedure, diagnoses, medications) from a claim or encounter as part of the data the payer makes available to satisfy the requirement for clinical data where the minimum expectation is USCDI and the exchange standard is FHIR R4 US Core profiles? Response: There is no prohibition. b. Is there a requirement to include such information to meet the final rule requirement for, at a minimum, clinical data represented in USCDI (e.g., Procedures, Medications)? i. In the member access API? ii. As part of Payer-Payer exchange at enrollee request? Response: In both cases, if the payer maintains data elements defined as part of the USCDI version 1, these data must be shared via the appropriate API or data exchange provision. 23-Jun-2020

With respect to information received via a claim or encounter: a. Response: There is no prohibition. b. i. & ii. Response: In both cases, if the payer maintains data elements defined as part of the USCDI version 1, these data must be shared via the appropriate API or data exchange provision.

1004 Unstructured data (PDF, images, etc) 4) Is data in PDF format considered electronic data for the purposes of meeting the requirements for enrollee access to clinical data via the API? Same question for Payer – Payer exchange? 23-Jun-2020

Response: The final rule does not define the number of endpoints payers must have. A payer may support one or more endpoints to implement the final rule requirements. The final rule also does not specify how each payer must approach making covered information available for covered products available through their API (s) (APIs). Generally speaking, as long as the enrollee's covered by this policy are able to obtain their data in the manner required, how the API endpoints are operationalized is not a factor. For details about the USCDI version 1 definition of maintain, the data are part of the enrollee's record, and within current status of the USCDI data elements maintained. Per the final rule, the payer but are not currently in a FHIR format, these data would need to be converted to a FHIR format and shared via the Patient Access API. The Payer-to-Payer exchange does not require the use of a FHIR format starting in 2022, though we strongly encourage exchange via a FHIR API as these data will be prepared to share via this format for the Patient Access API requirements. Under the current Payer-to-Payer provision, this could be an exchange of PDF records.

Update: See Response to Question Number CMS Final Rule Questions and Answers log#6016 and CMS Final Rule Questions and Answers log#6016

1005 Unstructured data (PDF, images, etc) 5) Is data in image format (clinical images, scanned documents, etc.) considered electronic data for the purposes of meeting the requirements for enrollee access to clinical data via the API? Same question for Payer – Payer exchange?

13-Jul-2020

Response: Correct, at this time, access to information from any prior covered plan under the rule provided by the same payer is not required by the Patient Access API. The Patient Access API applies to a current enrollee's current coverage.
3) Please verify that providing access to information from prior covered plans covered under the rule provided by the same payer does not violate the final rule provisions for the Patient Access API.

Response: The Interoperability and Patient Access final rule does not prohibit payers from providing information from prior covered plans as part of patients request for information. If a payer maintains information for an enrollee from multiple lines of business and wishes to include that information, that is permissible. The final rule requirements set the minimum, but payers can include this additional information. 14-Jul-2020

10-Aug-2020

4) Please verify that providing access to information from coverages (e.g., dental, vision) provided by the same payer that are not of a plan covered under the rule does not violate the final rule provisions for the Patient Access API.

Response: All claims information, including dental and vision services, that are part of an enrollee’s current plan, if that plan is impacted by the final rule, must be made available via the Patient Access API. As noted above, if the payer provided services to an enrollee previously under a different plan, the information from that previous plan is not required, though also not prohibited, to be shared.

See also CMS Final Rule Questions and Answers log#6023.

14-Jul-2020

5) Please verify that the member’s use of OAuth 2.0 and Open ID Connect meet all of the requirements for an electronic signature or ‘written’ approval for release of information that may be required by HIPAA and/or SAMHSA.

Response: 42 CFR Part 2 requires specific consent to be obtained for certain types of information. That requirement is not in any way impacted by the policies in the CMS Interoperability and Patient Access final rule. All existing federal, state, and local laws that require additional consent for specific types of information are not impacted by this final rule and must be adhered to. Regarding consent for health information not covered by regulations such as 42 CFR part 2, yes, the OAuth 2.0 authorization framework as specified in the ONC 21 st Century Cures Act final rule, which is adopted as part of the requirements under the CMS Interoperability and Patient Access final rule, requires the patient to formally authorize/approve for a third-party (an application) to receive data on behalf of a patient for a limited period of time, before the third-party is able to receive data using the specified API. The “authorization” part could be considered or seen as an electronic signature “process” executed by the patient with the intent to sign the data that is made accessible to the application, for the duration of time that the authorization is valid. As such, we do not believe an additional consent process is necessary for this information for this specific use.

14-Jul-2020

6) Please verify that current laws, such as 42 CFR part 2 and relevant state laws restricting access to specific information (additional protected data) must still be met to release this information in addition to the authorization by the member to release their other data to a third-party application.

Response: Yes, payers must comply with current laws such as HIPAA Privacy and Security rules, relevant state laws, and 42 CFR part 2 as applicable to access and release specific information.

14-Jul-2020

7) Please verify that all data (e.g., claims, clinical data) not restricted by current laws (such as 42 CFR part 2 and relevant state laws) must be made available to a third-party application at the member’s request.

a) Please verify that any OAuth scope statement may only be restricted to the individual and not to the data on that individual.

Response: See response to question 7b below.

Response: Yes.

Response: The final rule requires payers to make all the specified data available via the Patient Access API. Payers are not required to provide additional options to segment data or otherwise provide an opportunity to opt in or out of sharing certain FHIR resources or data elements. When a patient authorizes an app of their choice to retrieve their data from their health plan, the expectation is all available claims/encounter and clinical data is being made available. Regarding an OAuth scope statement, the inquirer may be referencing the ONC 21st Century Cures Act final rule regarding requirements for Certified EHR Technology (CEHRT), For more information on that, see 85 CFR 25741. Those ONC requirements are specific to CEHRT and are not related to the CMS Interoperability and Patient Access final rule.

14-Jul-2020

1. The preamble of the CMS Final Rule reads as follows: “If the patient requests their data via the Patient Access API from a payer, the payer must make available all of the data allowed per current law, such as 42 CFR part 2 and relevant state laws, including the data as specified in this final rule. We reiterate, however, that the data that are available to be shared are only to be shared at the patient’s request. If there are data elements the patient does not want to be shared, they can choose not to make the request. In addition, we note that this policy allows data to be exchanged from the payer to a third-party app of the patient’s choice for their personal use. This rule does not require any data exchange directly between or with providers.”

1.a) While the rule does not require any data exchange directly with providers, does the rule allow such an exchange (e.g., can the third-party application be a provider’s technology, such as the provider’s EHR)?

Response: The CMS Interoperability and Patient Access final rule, requires the patient to authorize an app of their choice to retrieve their data from their health plan, the expectation is all available claims/encounter and clinical data is being made available. We have four questions regarding the above quote from the final rule:

b) Does this indicate that data shared at patient’s request must include data normally requiring specific release by the patient (e.g., 42 CFR part 2 or based on specific state laws), without additional authorization by the patient, through the Patient Access API? Does this imply that the patient may only share all or nothing with a third-party application?

c) Alternatively, may the payer require amendment to the additional patient permission to release this additionally protected data (e.g., 42 CFR part 2 and relevant state laws) to the third-party application as per the payer’s normal policy?

d) For data, other than additionally protected information (e.g., 42 CFR part 2 and relevant state laws), may the payer provide the ability for the patient to restrict specific information based on patient preference consent?

e) May the patient authorize the payer to only allow a specific third-party application to receive a specific sub-set of their information (e.g., allow access to claims data but not clinical data)?

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: A third-party application, per the final rule, is an application that the patient can use to access their personal health information. A patient does not have access to a provider’s EHR, so this would not be consistent with the requirements of the final rule.

10-Aug-2020

1. The preamble of the CMS Final Rule reads as follows: “If the patient requests their data via the Patient Access API from a payer, the payer must make available all of the data allowed per current law, such as 42 CFR part 2 and relevant state laws, including the data as specified in this final rule. We reiterate, however, that the data that are available to be shared are only to be shared at the patient’s request. If there are data elements the patient does not want to be shared, they can choose not to make the request. In addition, we note that this policy allows data to be exchanged from the payer to a third-party app of the patient’s choice for their personal use. This rule does not require any data exchange directly between or with providers.”

1. a) While the rule does not require any data exchange directly with providers, does the rule allow such an exchange (e.g., can the third-party application be a provider’s technology, such as the provider’s EHR)?

Response: The CMS Interoperability and Patient Access final rule, requires the patient to authorize an app of their choice to retrieve their data from their health plan, the expectation is all available claims/encounter and clinical data is being made available. We have four questions regarding the above quote from the final rule:

b) Does this indicate that data shared at patient’s request must include data normally requiring specific release by the patient (e.g., 42 CFR part 2 or based on specific state laws), without additional authorization by the patient, through the Patient Access API? Does this imply that the patient may only share all or nothing with a third-party application?

c) Alternatively, may the payer require amendment to the additional patient permission to release this additionally protected data (e.g., 42 CFR part 2 and relevant state laws) to the third-party application as per the payer’s normal policy?

d) For data, other than additionally protected information (e.g., 42 CFR part 2 and relevant state laws), may the payer provide the ability for the patient to restrict specific information based on patient preference consent?

e) May the patient authorize the payer to only allow a specific third-party application to receive a specific sub-set of their information (e.g., allow access to claims data but not clinical data)?

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:

2. The preamble citation and questions 1. (a.b.c.d.e) were covered in a group conversation with CMS on 10-July-2020.

Response: (1.b.c.d.e): We have four questions regarding the above quote from the final rule:
1. The final rule requires that we share information we maintain.

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule, including State Medicaid programs, has outsourced certain benefits management and claims processing, the requirements of the final rule still apply to them. For example, a Medicaid beneficiary should be able to find an app of their choice and authorize that app to retrieve their data via the Patient Access API. The identity of the business associate, outsourced entity, or benefit manager is not relevant. It is the responsibility of the State to ensure it a beneficiary covered by them is able to request the specified data. See 85 FR 25532 for further discussion on this point.

2. We are assuming that the FHIR access scope, given to the apps, is "patient" read. This is particularly important in terms of how we will support access to data for a minor dependent or for access by a personal representative to the person/people they represent. The implication is that the consent flow will require the user to select the person who's data they are connecting the app to (it could be their own, if a minor, a minor dependent or a person that they are a personal representatives for). The alternative (some sort of new user scope for multiple patients) does not look to have any convention that can be adopted, without complicating the work for apps.

Response: If an organization impacted by the Interoperability and Patient Access final rule, including State Medicaid programs, has outsourced certain benefits management and claims processing, the requirements of the final rule still apply to them. For example, a Medicaid beneficiary should be able to find an app of their choice and authorize that app to retrieve their data via the Patient Access API. The identity of the business associate, outsourced entity, or benefit manager is not relevant. It is the responsibility of the State to ensure it a beneficiary covered by them is able to request the specified data. See 85 FR 25532 for further discussion on this point.

3. State Medicaid and others have asked that if they have "outsourced" to the enrollee's authorized third-party application (EOB, USCDI) may exchange the designated minimum data regarding an admission, discharge or transfer by any electronic method and not just by using HL7 V2 messaging.

Response: If data covered by USCDI is in PDF or image format, does making it available 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.

4. It is defined 45 CFR 170.205(d); it is correct that this requirement does not require the use of a specific standard to share the electronic notification. We did not propose, and thus did not finalize, a specific format or standard for the patient event notification that a hospital would be required to send under the proposed CoP. Thus, hospitals would be allowed to transmit patient event notifications using other standards, such as the CCDA or via a FHIR-based API (see 85 FR 25596 through 25597).

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule should be directed to the Office of the National Coordinator at For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

5. We are continuing to evaluate this question. (10-Aug-2020)

Response: If an organization impacted by the Interoperability and Patient Access final rule, including State Medicaid programs, has outsourced certain benefits management and claims processing, the requirements of the final rule still apply to them. For example, a Medicaid beneficiary should be able to find an app of their choice and authorize that app to retrieve their data via the Patient Access API. The identity of the business associate, outsourced entity, or benefit manager is not relevant. It is the responsibility of the State to ensure it a beneficiary covered by them is able to request the specified data. See 85 FR 25532 for further discussion on this point.

6. To the enrollee's authorized third-party application (EOB, USCDI) may exchange the designated minimum data regarding an admission, discharge or transfer by any electronic method and not just by using HL7 V2 messaging.

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule should be directed to the Office of the National Coordinator at For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

7. We are continuing to evaluate this question. (10-Aug-2020)

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule should be directed to the Office of the National Coordinator at For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

8. Include API, Organization Type

Response: Information Blocking is beyond the purview of the CMS Interoperability and Patient Access final rule. For questions related to information blocking, refer to the Office of the National Coordinator's webpage and InfoGraphic which provides a summary: https://www.healthit.gov/topic/information-blocking. For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

9. Include API, Organization Type

Response: The CMS Interoperability and Patient Access final rule requirements apply to the payers indicated in the final rule. The data that these payers must make available depends on how the payer maintains the data.

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule should be directed to the Office of the National Coordinator at For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

10. Include API, Organization Type

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule should be directed to the Office of the National Coordinator at For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

11. Include API, Organization Type

Response: The CMS Interoperability and Patient Access final rule requirements apply to the payers indicated in the final rule. The data that these payers must make available depends on how the payer maintains the data.

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule should be directed to the Office of the National Coordinator at For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.

12. Include API, Organization Type

Response: The CMS Interoperability and Patient Access final rule requirements apply to the payers indicated in the final rule. The data that these payers must make available depends on how the payer maintains the data.

Response: Questions specific to obligations under the ONC 21st Century Cures Act final rule should be directed to the Office of the National Coordinator at For additional assistance on the ONC rule, send questions to the ONC feedback form: https://www.healthit.gov/form/healthit-feedback-form.
4011 Patient Access API, Information Blocking, and Organization Type

4. If a payer chooses not to implement a suggested IG (such as CARIN BB or PDx Plan Net) and subsequently adopts their own proprietary IG, does this constitute data blocking?

ANSWER: The CMS Interoperability and Patient Access final rule does not require the use of any specific Implementation Guides. That said, the implementation guides suggested provide information payers can use to meet the requirements of the policies finalized in the rule without having to develop an approach independently, saving time and resources. In addition, the reference implementations made available for this IG allow payers to see the APIs in action and support testing and development. We note that the rule does require payers to make documentation about their API publicly and freely available as not to inhibit a third-party app from accessing the IG at an enrollee’s request. Ultimately, we do strongly encourage payers to consider using the suggested IGs. For questions related to information blocking and impacted organizations, refer to the Office of the National Coordinator’s webpage and Infographic which provides a summary: https://www.healthit.gov/topic/information-blocking

4012 Patient Access API, Information Blocking, and Organization Type

5. If an application vendor (such as Apple HealthKit) adopts the CARIN IG as the method for patient administrative data intake, as recommended by CMS, does every payer need to accommodate that application vendor’s decision to use the CARIN IG?

ANSWER: The CMS Interoperability and Patient Access final rule requires impacted payers to make certain information available via a FHIR-based API. Third-party vendors can leverage these types of data and offer their apps to patients. A compliant payer API will have the necessary data available in the specified FHIR format, and the payer will have the required API documentation publicly available. This will permit third-party apps to accommodate patient requests to retrieve their data from impacted payers. The final rule does not include requirements for third-party vendors.

5001 Payer to Payer Retention Policy

1. Are there any conditions under which the January 1, 2016 date is not applicable?

2. If normal payer retention policies make data subsequent to January 1, 2016 not maintained by CMS definition?

3. If a current payer translates information received from a prior payer at member request and exceeds the current payer’s retention policy?

ANSWER: Yes. An impacted payer is only required to maintain and send data into FHIR to a subsequent payer. The CMS Interoperability and Patient Access final rule requires payers to incorporate data they receive from another payer into their enrollee’s record. However, a payer is only required to send the data received under the payer-payer exchange requirement. There is no prohibition on exchanging the data received from a prior payer in a FHIR format. We do encourage payers to consider sending and receiving these data via an API, and we did note in the final rule that we may consider for future rulemaking an API-based payer-to-payer data exchange (85 FR 25567).

5002 Payer to Payer

2. If the current payer receives information from a prior payer at member direction, is the current payer required to maintain the information in the format(s) it was received and exchange it with a subsequent payer in the same format(s)?

ANSWER: Yes. An impacted payer is only required to maintain and send data received under this payer-to-payer data exchange requirement in the electronic form and format it was received. In this way, a payer would not be asked to receive paper records from another payer under this policy and then in turn share those paper records with another payer in the future at the patient’s direction. If the payer received an enrollee’s information via an API, the payer must share it via an API the payer are sending it to has the capacity to receive it (85 FR 25567).

5003 Payer to Payer

3. If a current payer translates information received from a prior payer into FHIR resources and makes those FHIR resources available to a subsequent payer, does this meet the requirement of the rule?

ANSWER: Yes. The Interoperability and Patient Access final rule only requires payers to receive and maintain data in the form and format it was received under the payer-payer exchange requirement. There is no prohibition on exchanging the data received from a prior payer in a FHIR format. We do encourage payers to consider sending and receiving these data via an API, and we did note in the final rule that we may consider for future rulemaking an API-based payer-to-payer data exchange (85 FR 25567).

5004 Payer to Payer

4. Is the current payer allowed to exchange the data received from a prior payer in the original format and a translation of any part of those data into FHIR to a subsequent payer?

ANSWER: Yes. This is recommended by CMS, although not prohibited from doing so.

5005 Payer to Payer

5. If a covered plan maintains data derived from clinical or claims data that meets the USCDI definitions, but is solely generated by the payer, do those data need to be made available via the Patient Access API and exchanged via the Payer-to-Payer requirement?

ANSWER: Yes. The Interoperability and Patient Access final rule requires payers to incorporate data they receive from another payer into their enrollee’s record to determine whether it fits within the criteria. As such, the payer now maintains that data, and must provide it to the enrollee as part of the patient record to determine whether it fits within the criteria.

5006 Payer to Payer

6. In the patient-directed exchange between a prior payer and the designated recipient payer, can the “send data requirement” be met by giving the designated recipient payer access to the API for clinical data (USCDI) that is used for enrollee designated third-party applications?

ANSWER: Yes. The Interoperability and Patient Access final rule does not specify the means by which payers conduct the exchange of electronic information between payers under the Payer-to-Payer Data Exchange. As noted above, we do encourage payers to consider leveraging an API for this data exchange. As the method of electronic data exchange is not specified, there are no specific requirements around FHIR resources. We do encourage payers to consider using those FHIR resources that will make the data most valuable to other payers and ultimately patients over time.

5007 Payer to Payer

7. Will CMS FFS participate in the exchanges defined by the CMS final rule?

a) Can Medicare FFS receive data from another payer at the direction of the enrollee?

b) Will CMS provide information received from another payer at the direction of the enrollee, along with any USCDI maintained by CMS, to another payer at the direction of the beneficiary?

ANSWER: Yes. The Interoperability and Patient Access 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). We encourage each payer to look at how they maintain the data as part of the patient record to determine whether it fits within the criteria.

6001 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?

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

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?

28-Jul-2020

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.

09-Nov-2020

Patient Access

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 not to include the information in the Patient Access API is this considered data blocking?

28-Jul-2020

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 such, these data would need to be shared, there are no implications for information blocking.

09-Nov-2020

Duplicate data

If a payer has the same information available from multiple sources (claims, CCR, ORUs) 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?

28-Jul-2020

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 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.

09-Nov-2020

Security Information Blocking

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?

28-Jul-2020

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. The process for a payer to determine when to block access to third-party applications includes the following steps:

1. The payer will identify the criteria to be used to determine when to block access to third-party applications.
2. The payer will determine if a third-party application is suspected of violating its security policies.
3. The payer will investigate the application to determine if it is in violation of its security policies.
4. If the application is found to be in violation of its security policies, the payer will terminate the application’s access to the API.

09-Nov-2020

Processing Adjudication

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. the answer impacted if the payer only processes claims periodically (e.g. once a week)?

28-Jul-2020

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 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 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).

09-Nov-2020

Provider Directory Security

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?

28-Jul-2020

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 is not PHI, and generally publicly available information at this time, restrictions are not permitted (see 85 FR 25564 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.

09-Nov-2020

USCDI risk adjustment

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 it was obtained through clinical data sources such as CDA documents and ORU result messages?

28-Jul-2020

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, controls 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.

09-Nov-2020
partner

contract

maintain

While the directory data for a covered payer is required to be openly available, 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) 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 USCDI data elements contained in it to FHIR and maintain as part of an enrollee's record as a DocumentReference resource to make the unstructured data available via the Patient Access API. The final rule does require that the formulary data specific to the patient in question be made 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.

Payers require, from a security and audit perspective, that the designated third-party application must use the OAuth 2.0 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 representative" 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 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 https://www.hhs.gov/hipaa/forprofessionals/faq/2069/under-hipaa-when-can-alternate-member/index.html.

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.

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. There is no prohibition in the rule to making the formulary service when integrated with protected health information (PHI) 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 USCDI data elements contained in it to FHIR and maintain as part of an enrollee's record as a DocumentReference resource to make the unstructured data available via the Patient Access API. 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.

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 OR the relationship between the representative and the beneficiary. 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).

The expectation is that the payer will maintain a protected resource server, which will be looking for a token from the provider to act on behalf 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 by itself or by interacting with a separate identity server. Either way, a screen (or series of screens, if necessary) can be displayed where the provider has access to (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 in 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 of 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.

The expectation is that the payer will maintain a protected resource server, which will be looking for a token from the provider to act on behalf 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 by itself or by interacting with a separate identity server. Either way, a screen (or series of screens, if necessary) can be displayed where the provider has access to 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 in 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 of 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.

Payers require, from a security and audit perspective, that the designated third-party application must use the OAuth 2.0 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 representative" 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 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 https://www.hhs.gov/hipaa/forprofessionals/faq/2069/under-hipaa-when-can-alternate-member/index.html.

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.

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. There is no prohibition in the rule to making the formulary service when integrated with protected health information (PHI) 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 USCDI data elements contained in it to FHIR and maintain as part of an enrollee's record as a DocumentReference resource to make the unstructured data available via the Patient Access API. 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.
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 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 Plan A and Plan B) via the Patient Access API with any duplication of data included?

25-Aug-2020

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.

09-Nov-2020

With respect to the term adjudication in final rule, is it CMS's intent that the process is complete (e.g. starts the 1 business day clock) when the claim processing is finished or when the provider payment process is complete? 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?

25-Aug-2020

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, 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.

09-Nov-2020

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 5 months (see 85 FR 25746).

09-Nov-2020

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 json 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) that is (this is standard industry approach today).

25-Aug-2020

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 that are 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 otherwise be easily found by any 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).

09-Nov-2020

Can EHR vendors prevent payers from using a SMART on FHIR app if they don't have a place to hold pharmacy count and mix in the return the pharmacy information to the requester. FHIR's Bundle does not provide the most useful information. Do NUCC taxonomy codes fulfill the intent of "mix"?

Car 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/cureact/

09-Nov-2020

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 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.

09-Nov-2020

Pharmacy Directory

The regulation states the following for MA-PD plans

For an MA organization that offers an MA-PD plan, the MA-PD's pharmacy directory, including the pharmacy name, address, phone number, number of pharmacies in the network, and mix (specifically the type of pharmacy, such as 'retail pharmacy' that could be interpreted as retail vs inpatient, or as the pharmacy variants in NUCC Provider Taxonomy (e.g., retail vs inpatient vs long term care vs others). We believe the NUCC codes will provide the most useful information. Do NUCC taxonomy codes fulfill the intent of "mix"?

Additional Clarification Question:

The DaVinci Plan-Net IG uses a FHIR construct known as a 'Bundle' to return the pharmacy information to the requester. FHIR's Bundle does not support summary information such as pharmacy count and mix. We don't have a place to hold pharmacy count and mix in the response. The simplest alternative for the requester to determine the count and mix is to use the FHIR response. This is simple to determine and is only necessary if count or mix is useful for the consumer using their app.

02-Mar-2021

MA organizations that offer MA-PD plans must make available, at a minimum, pharmacy directory data and include the pharmacy name, address, phone number, number of pharmacies in the network, and mix. MA-PD plans should build a Provider Directory API that will provide information for beneficiaries to enable them to find appropriate pharmacy services. This would include the location, phone number, and the designation or type of pharmacy (e.g. retail, compounding, etc.) for all pharmacies accessible via an API. See 85 FR 25604 and 25633.

Patients may use the taxonomy codes suggested by the Implementation Guide, if applicable, or NUCC if they determine that taxonomy is appropriate for their purposes. To the extent practicable, standardization across implementers would be appropriate.

Additional Clarification Question:

MA-PD plans are encouraged to build a Provider Directory API that is conformant to the Plan-Net Implementation guide, and that will provide information for beneficiaries to enable them to find appropriate pharmacy services. We have encouraged payers to use certain implementation guides and reference implementations. As we have continued to reiterate, conformance to this suggested Plan-Net IG will address the requirements for a Provider Directory API for pharmacy directory data.

02-Mar-2021
Patient Access API

The preamble to the rule mentions both “Designated Record Set” and Clinical data as defined by UCSID V1.0.

a. Is the requirement to provide clinical data as defined by the HIPAA designated record set or by OCR's UCSID V1.0?
b. If the information is used for no other purpose?
c. If the information is used to report Gaps in Care to the Provider?

The Interoperability and Patient Access 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). All UCSID data that the payer maintains as part of the enrollee record are to be made available via the Patient Access API. The answer to which data are to be made available depends on how each payer maintains data. It is up to each payer to evaluate how data are maintained in its systems for each enrollee. (Similar question was asked and answered in October 2020)

02-Mar-2021

Payer-to-Payer

Please confirm that if a payer implements the payer-to-exchange as defined in the Da Vinci Payer Data Exchange (PDex) Implementation Guide, it satisfies the Payer-to-Payer exchange requirement defined in the CMS Interoperability Final Rule that must be supported by covered plans by 1/1/2022.

As finalized in the Interoperability and Patient Access final rule, payers are allowed multiple methods for electronic exchange of the required patient-identified exchange (between payers), which could include the payer-to-payer exchange as defined in the Da Vinci Payer Data Exchange (PDex) Implementation Guide (IG). The PDex IG meets the requirement of the rule to enable the exchange of the UCSID version 1 and would satisfy the Payer-to-Payer exchange requirement that must be supported by covered plans by 1/1/2022, as long as it is implemented in accordance with other relevant requirements of the rule. Payers may also choose other means by which to exchange data if requested by the patient. While CMS did not specify the use of a particular IG in the May 2020 interoperability rule, we do encourage the use of standards. (85 FR 25565).

22-July-2021

Since the CMS Interoperability Final Rule requires that payers must support enrolled or prior members of covered plans' ability to exchange copies of their records (at least for UCSID V1) with the new payer, can the payer consider this to be part of operations as defined by OCR?

Background: The CMS Interoperability Rule established a coordination of care transaction to communicate between plans that is triggered by an enrollee's request for information about them held by a payer to be sent or received and incorporated into their records held by the receiving payer. Payers subject to this requirement must maintain a process for the electronic exchange of, at a minimum, the data elements in the UCSID. Payers must use this process to exchange the UCSID defined set data set with the approval and at the direction of a current or former enrollee, or the enrollee's personal representative. The receiving payer must include these data in the record it maintains to such enrolee and make it available for individual enrollee access. While the obligation to incorporate data received from other payers into the receiving payer's records applies only for data about current enrollees, once incorporated, these data must be maintained even after a current enrollee leaves the payer's coverage.

- The HIPAA Privacy Rule permits a covered entity to disclose PHI to another covered entity for its own health care operations purposes, or for the health care operations of the entity receiving the information. If an individual had been enrolled in a health plan of Covered Entity A and switched to a health plan provided by Covered Entity B, Covered Entity A can disclose PHI to Covered Entity B to coordinate the individual's care, without the individual's authorization. See 3014-HIPAA and Health Plans – Uses and Disclosures for Care Coordination and Continuity of Care (HHS.gov).

22-July-2021

If the requirement for Payer-to-Payer exchange is part of operations as defined by OCR, does capturing the opt-in request of the enrolled member by the new plan for the new plan to obtain data from the member's prior plan meet all relevant consent requirements for both the new and prior payer?

The HIPAA Privacy Rule permits, but does not require, covered entities to obtain consent of the individual to use or disclose PHI for treatment, payment, and health care operations purposes. See FAQ 264 https://www.hhs.gov/hipaa/professionals/faq/264-what-is-the-difference-between-consent-and-authorization/index.html

22-July-2021

**** CMS DISCLAIMER ****

These responses were current at the time they were sent. 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 the 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.