### CMS Final Rule Questions and Answers log


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.

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Category</th>
<th>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></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 &quot;used&quot; the data. Payers frequently will not have knowledge of the actual data/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 xxx organization on xxxxx 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 exclude the provenance resource?</td>
<td>23-Jun-2020</td>
<td>Response: Appreciating the additional value the PDex IG provides for organizations, or interested parties.</td>
<td>13-Jul-2020</td>
</tr>
<tr>
<td>1002</td>
<td></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. If the payer is 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? e. If the member enrollee has access to all prior coverages 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 Payer 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 &quot;maintained&quot;. The final rule defines &quot;maintained&quot; 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 maintained 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 those maintained data are not currently in a FHIR format, those 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 &quot;maintains&quot; the data for the enrollee in their current plan. No, this is not required. Again, this goes back to how the payer &quot;maintains&quot; the data. c. Response: No, this is not required. Again, this goes back to how the payer &quot;maintains&quot; 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 years' data as part of the enrollee's current 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 based on FHIR R4 US Core profile? 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 API as appropriate or data exchange provision.

23-Jun-2020 With respect to information received via a claim or encounter:

a. Response: There is no prohibition.

b. 1. & 2. 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.

13-Jul-2020

4) Is data in PDF format considered electronic data for the purposes of meeting the requirements for enrollee access to clinical data via the member API? Same question for Payer – Payer exchange?

Response: Though the payer did not obtain the information through direct request, 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 for covered products available through their API or APIs.

23-Jun-2020 Response: As noted above, if the required data elements are maintained by 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 data 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.

13-Jul-2020

5. Is there any requirement in the final rule that would impact a payer's ability to access information about a covered or non-covered product?

Response: Correct, the Patient Access API is only required, at a minimum, to make available covered information for the covered plan in which the member is currently enrolled, data which is maintained by that current plan.

9-Jul-2020 Response: Though the payer did not obtain the information through direct observation, the payer is required to include the information in the Patient Access API or Payer-to-Payer data exchange if the payer maintains the data, control over the data, and authority to make the data available through the API (e.g., currency or completeness) of the USCDI data element. A payer is only required to provide the patient the opportunity to choose specific types or segments of this available data be shared or not shared.

10-Aug-2020

6. Are impacted payers required to share FHIR concept data for covered products available through their API or APIs?

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 for covered products available through their API or APIs.

9-Jul-2020 Response: As noted above, if the required data elements are maintained by 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 data 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.

13-Jul-2020

1. Is there a requirement for one API endpoint for all data or may a payer support multiple endpoints (e.g., one for EOB and another for USCDI data) to meet the requirements of the final rule?

Response: There is no need for a payer to provide access to covered information for more than one covered product (e.g., CHPP, MA, Medicaid, CHIP) through the same endpoint(s). Does answer/guidance change depending on organizational/legality structure providing products where multiple payers (e.g., different organizations for CHPP, MA, Medicaid, CHIP)?

5) Is there any requirement for one API endpoint for all data or may a payer support multiple endpoints (e.g., one for EOB and another for USCDI data) to meet the requirements of the final rule?

Response: If prior authorization is required, is a single indicator (e.g., Y/N) sufficient?

a) If prior authorization is required, is a single indicator (e.g., Y/N) sufficient?

b) Are there any data blocking implications if multiple patient access API endpoints are implemented as described in preceding questions?

9-Jul-2020 Response: If prior authorization is required, the status of covered drugs, tiering information, and utilization management requirements are recognized as part of the implementation of the Patient Access API. The Patient Access API applies to a current enrollee's or current coverage.

9-Jul-2020 Response: For the final rule, if a patient requests their data be made available to a third-party app via the Patient Access API, the patient is authorizing the payer to share all available data as specified in the final policy. This means all claims/exchange and clinical data in the form of the USCDI that the payer maintains with a date of service on or after January 1, 2016, as well as any data available, as required, under this policy.

10-Aug-2020

3. The rule suggests that FHIR patient data access scope should not be recognized as part of the implementation of the Patient Access API and that the only mode is ‘all data’ available (e.g., read?). Is this interpretation correct?

9-Jul-2020 Response: The rule specifies that FHIR patient data access scope should not be recognized as part of the implementation of the Patient Access API and that the only mode is ‘all data’ available (e.g., read?). Is this interpretation correct?

10-Aug-2020

4. Does the concept of data that payers ‘maintain’ require that the payer has current information available for a USCDI element (e.g., smoking status) or is the payer required to make any USCDI element available even if the data is known not to be current or to be incomplete?

9-Jul-2020 Response: The rule specifies that FHIR patient data access scope should not be recognized as part of the implementation of the Patient Access API and that the only mode is ‘all data’ available (e.g., read?). Is this interpretation correct?

10-Aug-2020

2. If outsourced benefit manager processes claims or maintains clinical data under delegation, may they provide the Patient Access API endpoint(s) for those specific services?

Response: The rule specifies that FHIR patient data access scope should not be recognized as part of the implementation of the Patient Access API and that the only mode is ‘all data’ available (e.g., read?). Is this interpretation correct?

9-Jul-2020 Response: The rule specifies that FHIR patient data access scope should not be recognized as part of the implementation of the Patient Access API and that the only mode is ‘all data’ available (e.g., read?). Is this interpretation correct?

10-Aug-2020

5. Is there any requirement in the final rule that would impact a payer’s standard data retention policy?

9-Jul-2020 Response: The rule specifies that FHIR patient data access scope should not be recognized as part of the implementation of the Patient Access API and that the only mode is ‘all data’ available (e.g., read?). Is this interpretation correct?

10-Aug-2020

6. As part of telephonic case management, payers may verbally acquire from the member information such as vital signs that are not obtained by clinical observation.

a) Is this type of information considered to be USCDI elements and therefore covered by the final rule requirement to make these data available (e.g., is member-reported data included under the rule)?

b. Is part of the Patient Access API requirement?

c. As part of Payer to Payer exchange requirement?

9-Jul-2020 Response: The rule specifies that FHIR patient data access scope should not be recognized as part of the implementation of the Patient Access API and that the only mode is ‘all data’ available (e.g., read?). Is this interpretation correct?

10-Aug-2020

7. Formulary

1) Does the rule require that a Formulary API includes an indicator of the status of covered drugs, listing information, and utilization management requirements?

a) If priority authorization is required, is a single indicator (e.g., Y/N) sufficient?

9-Jul-2020 Response: The rule requires that impacted payers, specifically MA-PD, Medicaid and CHIP managed care entities are required to make information about covered Part D drugs, and any tiered formulary structure or utilization management policy which pertains to those drugs (42 CFR 422.119(b) (2)(ii), Medicaid and CHIP FFS programs, Medicare managed care plans, and CHIP managed care entities make formularies or preferred drug lists available via the Patient Access API. MA organizations that offer MA-PD plans are specifically required to make available formulary data that includes covered Part D drugs, and any tiered formulary structure or utilization management policy to those drugs (42 CFR 422.119(b) (2)(ii), Medicaid and CHIP FFS programs, Medicare managed care plans, and CHIP managed care entities are required to make information about covered outpatient drugs and updates to such information, including, where applicable, preferred drug list information through the Patient Access API (see requirements under 42 CFR 431.60(b)(4), 438.233(b)(6), 457.233(b)(4), and 42 CFR 457.1233(d)(2)).

A. We suggest leveraging the PDAX Formulary V3 to meet these requirements. a) If priority authorization is required, a single indicator of Y/N is sufficient.

8-Jul-2020

3001 1) Please verify that the Patient Access API is only required to access covered information for the covered plan covered under the rule in which the member is currently enrolled.

14-Jul-2020 Response: Correct, the Patient Access API is only required, at a minimum, to make available covered information for the covered plan in which the member is currently enrolled, data which is maintained by that current plan.

10-Aug-2020

3002 2) Please verify that access to information from any prior covered plan covered under the rule provided by the same payer is not required by the Patient Access API (other than via Payer to Payer exchange at member request).

14-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.

10-Aug-2020
3003 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.

14-Jul-2020 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.

10-Aug-2020

3004 Dental Vision 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.

14-Jul-2020 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 not prohibited, to be shared.

10-Aug-2020

3005 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.

14-Jul-2020 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 21st 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.

10-Aug-2020

3006 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.

14-Jul-2020 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.

10-Aug-2020

3007 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 not to the data on that individual.

b. Regarding question 7, may the payer provide any additional options regarding release of the information other than all or none?

14-Jul-2020 Response: Yes. 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.d): See response to question 7b below.

Response: Yes. See response to 7b below.

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.

10-Aug-2020

3008 1. The preamble of the CMS Final Rule roads 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)?

14-Jul-2020 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

3009 1. The preamble of the CMS Final Rule roads 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.”

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 additional patient permission to release this additional 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?

14-Jul-2020 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.): Current law must be adhered to — such as 42 CFR part 2 and relevant state law. As stated in the final rule, "the policies finalized in this regulation do not change any payer or provider’s obligations to abide by existing federal and state regulations and law, including 42 CFR part 2, which governs certain substance use disorder records, which are some of the most sensitive health information. We note, however, that the patient can direct the entity to transfer this sensitive data upon their designation of a recipient, or may provide consent or authorization for the transfer, as applicable" (85 FR 25538).

Response (1.c): See response above (1.b) (2009).

Response (1.d): See response to question 7b above (CMS Final Rule Questions and Answers log#5007).

Response (1.a): See response to question 7b above (CMS Final Rule Questions and Answers log#5007).

10-Aug-2020
1. Is the Patient Access API intended to support consent for and access to medical data?
   a. The patient
   b. A member’s “representative” (as defined in the Rule) (patient advocate)
   c. Parent access to dependent child’s data
   d. Spouse access to member’s data
   e. POA access to member’s data, etc.
   f. Are third parties granted delegated access without bearing to the relationship between member and payer, rather relationship between member and the patient?

1. Are the elements of information covered by the Interoperability and Patient Access final rule, including those regulated by the ADT Sharing requirement, relevant to the Patient Access API?

1. Is the Patient Access API intended to support consent for and access to medical data?
   a. The patient
   b. A member’s “representative” (as defined in the Rule) (patient advocate)
   c. Parent access to dependent child’s data
   d. Spouse access to member’s data
   e. POA access to member’s data, etc.
   f. Are third parties granted delegated access without bearing to the relationship between member and payer, rather relationship between member and the patient?

Response: The CMS Interoperability and Patient Access final rule reiterated ADT Sharing response. If an organization impacted by the Interoperability and Patient Access final rule, we reiterated ADT Sharing response. If data sharing is already effectively occurring, the API is a new way to make the data available. We also said that the current regulation does not change existing privacy relationships between minors and parents. In most health plans, the policy holder has access to the claims and other information for other members covered by the policy, unless there is a privacy provision in place. We also referenced HIPAA Privacy Rule at 45 FR 164.522, which says that individuals have a right to request restrictions on how a covered entity will use and disclose protected health information. The final rule does not change any requirements under federal, state, local, or tribal law. Please see 85 FR 25547 for a more complete discussion of privacy and access as it relates to an enrollment group.

Response: The policy for the Patient Event Notification CoP requirement is limited to those hospitals and CAHs that utilize an electronic medical record system or other electronic administrative system with the capacity to generate information for electronic patient event notifications. The standard is defined 45 CFR 170.205(d)(2). 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 CDCA or via a FHIR-based API (see 85 FR 25596 through 25597).

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, does the API requirement still apply to them (the state agency) or can Medicaid direct the member to the outsourced entity and expect the outsourced entity (e.g., benefit manager) will accept the responsibility for compliance?

Response: The policy for the Patient Event Notification CoP requirement is limited to those hospitals and CAHs that utilize an electronic medical record system or other electronic administrative system with the capacity to generate information for electronic patient event notifications. The standard is defined 45 CFR 170.205(d)(2). 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 CDCA or via a FHIR-based API (see 85 FR 25596 through 25597).

Response: The policy for the Patient Event Notification CoP requirement is limited to those hospitals and CAHs that utilize an electronic medical record system or other electronic administrative system with the capacity to generate information for electronic patient event notifications. The standard is defined 45 CFR 170.205(d)(2). 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 CDCA or via a FHIR-based API (see 85 FR 25596 through 25597).

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

Response: The CMS Interoperability and Patient Access final rule requires 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 45 FR 25596 through 25597.

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 45 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 45 FR 25596 through 25597.
4011 Patient Access API, Information Blocking, and Organization Type

4. If a payer chooses not to implement a suggested IG (such as CARRI BB or PDxV Data Net) and subsequently adopts its 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 noted in section 1. The CMS Interoperability and Patient Access final rule requires payers to maintain all data received under the payer-to-payer data exchange in the electronic form and format it was received. 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 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.

10-Aug-2020

4012 Patient Access API, Information Blocking, and Organization Type

5. If an application vendor (such as Apple Healthkit) adopts the CARRI 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 CARRI 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.

10-Aug-2020

5001 Payer to Payer Retention Policy

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

Response: The Interoperability and Patient Access final rule requires impacted payers to make the specified data they maintain with a date of service on or after January 1, 2016 available per payer request. 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). 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.

10-Aug-2020

5002 Payer to Payer

2. If the current payer receives information from a prior payer at enrollee request, 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)?

Response: Yes. An impacted payer is only required to maintain and send data received under this payerto-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 if the payer is sending it to have the capacity to receive it (85 FR 25567).

10-Aug-2020

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?

Response: A payer is not required to translate information received under this payer-to-payer data exchange requirement to FHIR. However, a payer is not prohibited from doing so.

10-Aug-2020

5004 Payer to Payer

4. Is the current payer required to exchange the data received from a prior payer into the original format and format it was received under the Payer-to-Payer requirement?

Response: No. If a payer received data from another payer in a format other than FHIR, the payer must share it via an API if the payer they are sending it to has the same API that meets the USCDI definitions, but is solely generated by the payer, as part of the patient record to determine whether it fits within the criteria.

10-Aug-2020

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?

Response: If a covered plan maintains USCDI data as part of an enrollee’s record, those data should be made available via the Patient Access API and payer-to-payer requirements.

10-Aug-2020

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? a) If data has been received from a prior payer in a format other than FHIR, can the data be exchanged by a separate method or made available through a FHIR DocumentReference resource? b) If the receiving payer utilizes the FHIR API to receive the data in the format it was received under the Payer-to-Payer requirement?

Response: No. If a payer received data from another payer in a format other than FHIR, the final rule requires payers to incorporate data they receive from another payer into their enrollee record. However, a payer is only required to send data received under the payer-to-payer data exchange in the electronic form and format it was received (85 FR 25567).

22-July-2020

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? Will this capability exist for 5 years after the beneficiary leaves Medicare FFS?

Response: The Medicare Fee-for-Service (FFS) program, although not required under the Interoperability and Patient Access final rule, is developing the capability to receive data from other payers at the direction of the enrollee as part of its modernization initiative. Generally, Medicare FFS is working toward meeting the requirements as stated in the final rule for the benefit of its beneficiary population even through not required to do so.

10-Aug-2020

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?

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

09-Nov-2020
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 PHR-based API under this payer to payer data exchange provision, and then the enrollees 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

If a payer receives data from a current enrollee’s former payer via a PHR-based API under the payer-to-payer data exchange provision, and then the enrollees 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. As these data would need to be shared, there are no implications for information blocking.

09-Nov-2020

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 event 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 or 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, information only needs to be mapped to PHR 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.

09-Nov-2020

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? Certain EHR vendors charge over $20,000 and an annual maintenance or usage fee.

28-Jul-2020

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

09-Nov-2020

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 plan 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 or disconnect. The 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)(8)(ii)(A)). NIST makes a number of tools available to assess risk (For more information, see https://www.nist.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/nist/800-53).

09-Nov-2020

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?

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 have 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)(8)(ii)(A)). NIST makes a number of tools available to assess risk (For more information, see https://www.nist.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/nist/800-53).

09-Nov-2020

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” mean the next business day or the business day following the next business day?

28-Jul-2020

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 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.

09-Nov-2020

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 endpont must be made publicly accessible. Specifically, the rule requires payers make the Provider Directory API accessible via a public-facing digital endpoint on their websites 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 the 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.

09-Nov-2020

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 access to 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
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. 30-Jul-2020 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. 09-Nov-2020

Patient Access Security OAuth OpenID SMART on FHIR authentication
If a covered payer requires an application that wishes to access the Patient Access API to meet specific industry standard requirements for same authentication and authorization, this 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 and OpenID Connect to ensure that an application will not present a risk to the payer systems, does this violate the CMS final rule? 06-Aug-2020 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/hipaasupportprofessionals/tg/2069/under-hipaa-when-can-affinity-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. 09-Nov-2020

Patient Access API Security OAuth token representative
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 representative” cannot be granted the ability to use another individual’s (e.g., the member’s) token. The payer 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? 06-Aug-2020 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 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 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 payer’s 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. 09-Nov-2020

consent credential token authorization authentication identity
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? 06-Aug-2020 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 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 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 payer’s 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. 09-Nov-2020

representative
Confirm that within the context of the rule, a representative is not maintained by the payer? 06-Aug-2020 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. (CMS Final Rule Questions and Answers log#6013) 09-Nov-2020

unstructured data pdf discrete data element parse DocumentReference
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 data. The Provenance of the FHIR output in Payer-to-Payer, to document 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). 25-Aug-2020 Regarding unstructured data such as a large PDF or a scan of a fax that may or may not include protected health information (PHI), 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 health record. This does not include 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 so as 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 patients to include these large files in the data available via the API. 09-Nov-2020
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 A has Plan B'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 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?

With respect to the term adjudication in final rule, is FHIR'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?

How long does a covered payer have to register a third-party application before it can be used to access the Patient Access API?

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 payer 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 protect 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?

Can EHR vendors prevent payers from using a SMART on FHIR app that would provide a patient summary of information at the point of care? Can EHR vendors prevent payers from using a SMART on FHIR app that would provide a patient summary information that would reduce work for the provider?
The CMS Interoperability Rule established a coordination of Payer-to-Payer transactions to support the exchange of designated record sets and clinical data as defined by USCDI V1.0. Individuals may send additional questions to the CMS Health Informatics and Interoperability Group (HIIG) at CMS_HealthInformaticsOffice@cms.hhs.gov.

The Interoperability and Patient Access final rule defines “maintain” to mean that the payer has access to the data, control over the data, and authority to make the data available through the API (85 FR 25530). All USCDI 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 who each payer maintains data. It is up to each payer to evaluate how data are maintained in its systems for each enrollee. (A similar question was asked and answered in October 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 processing actions before the payer has control over the data. It does not require payers to change their contractual relationships or current pre-processing procedures, though we strongly encourage payers and vendors to work together to make patient data available in a timely manner as possible. (Note, a similar question was asked and answered in October 2020)

The USCDI v1.0 includes the required content and vocabulary standards adopted at 45 CFR 170.213, and these are the data elements that must be provided through the Patient Access API if maintained in the payers system. The Interoperability and Patient Access final rule requires the minimum content to be adjudicated claims (including cost); encounters with capitated providers; provider remittances; enrollee cost-sharing; and clinical data, including laboratory results (where maintained by the payer). Payers must provide the clinical data they maintain, and over which they have control, in accordance with the standards available in the current version of the USCDI. The USCDI v1.0 includes the required content and vocabulary standards adopted at 45 CFR 170.213, and these are the data elements that must be provided through the Patient Access API if maintained in the payers system. The HIPAA designated record set is defined at 164.501 as (1) a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) The term record means any item, collection, or grouping of information that includes protected health information and is maintained, or collected, used or disseminated by or for a covered entity.

The Interoperability and Patient Access final rule mentions both “Designated Record Set” and Clinical data as defined by USCDI V1.0. a. Is the requirement to provide clinical data as defined by the HIPAA designated record set or by ONC’s USCDI V1.0?

The preamble to the rule mentions both “Designated Record Set” and Clinical data as defined by USCDI V1.0. a. Is the requirement to provide clinical data as defined by the HIPAA designated record set or by ONC’s USCDI V1.0?

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 processing actions before the payer has control over the data. It does not require payers to change their contractual relationships or current pre-processing procedures, though we strongly encourage payers and vendors to work together to make patient data available in a timely manner as possible. (Note, a similar question was asked and answered in October 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 processing actions before the payer has control over the data. It does not require payers to change their contractual relationships or current pre-processing procedures, though we strongly encourage payers and vendors to work together to make patient data available in a timely manner as possible. (Note, a similar question was asked and answered in October 2020)

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 USCDI V1) with the new payer, can the payer consider this to be part of operations as defined by OCR?

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 Interoperability and Patient Access final rule requires the minimum content to be adjudicated claims (including cost); encounters with capitated providers; provider remittances; enrollee cost-sharing; and clinical data, including laboratory results (where maintained by the payer). Payers must provide the clinical data they maintain, and over which they have control, in accordance with the standards available in the current version of the USCDI. The USCDI v1.0 includes the required content and vocabulary standards adopted at 45 CFR 170.213, and these are the data elements that must be provided through the Patient Access API if maintained in the payers system. The HIPAA designated record set is defined at 164.501 as (1) a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) The term record means any item, collection, or grouping of information that includes protected health information and is maintained, or collected, used or disseminated by or for a covered entity.