Questions originating from group conversation with Denise St. Clair, CMS, on 11-July-2020 (as follow up to a preceding HL7 WG discussion)

Note to Da Vinci Steering Committee: August 8, 2020.

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.

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. 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.
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). 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.
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 version 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.
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 21st 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.

6) Please verify that current laws, such as 42 CFR part 2 and relevant state laws restricting access to specific information (additionally 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.

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. Response: Yes.

    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 7b below.

    b. Regarding question 7, may the payer provide any additional options regarding release of the information other than all or none? 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. These ONC requirements are specific to CEHRT and are not related to the CMS Interoperability and Patient Access final rule.

General Question (based on review of Personas, introduced 09-July-2020, reviewed 14-July-2020)

The preamble citation and 4 of 5 original questions were covered by addition of questions generated by a group conversation with CMS on 11-July-2020. The remaining question below did not achieve consensus to be included in questions to submit to CMS (reviewed 14-July-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**, i**ncluding 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."

    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: 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.

    We have five 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? Response: 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).
    a) Alternatively, may the payer require/permit 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? Response: See response above.
    b) 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? Response: See response to question 7b above.

Commented [GM1]: Personas accuracy relevant to IG. Is there server(s) overhead? Is there variance of sub part c and e?

c) 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: See response to question 7b above.

Commented [GM2]: 4 of 5 original questions regarding the cited preamble were covered by addition of questions generated by a group conversation with CMS on 11-July-2020. These can be removed.