

CMS Advancing Interoperability and Improving Prior Authorization Processes proposed rule (CMS-0057-P) Comment

This document is submitted by the Massachusetts Health Data Consortium (MHDC) and its Data Governance Collaborative (DGC) in response to the CMS Advancing Interoperability and Improving Prior Authorization Processes Proposed Rule (CMS-0057-P) posted in the Federal Register on December 13, 2022 and found here: <https://www.federalregister.gov/documents/2022/12/13/2022-26479/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-advancing-interoperability>

About MHDC

Founded in 1978, MHDC, a not-for-profit corporation, convenes the Massachusetts's health information community in advancing multi-stakeholder health data collaborations. MHDC's members include payers, providers, industry associations, state and federal agencies, technology and services companies, and consumers. The Consortium is the oldest organization of its kind in the country.

MHDC provides a variety of services to its members including educational and networking opportunities, analytics services on both the administrative and clinical side (Spotlight), and data governance and standardization efforts for both clinical and administrative data (the Data Governance Collaborative/DGC and the New England Healthcare Exchange Network, respectively).

About DGC

The DGC is a collaboration between payer and provider organizations convened to discuss, design, and implement data sharing and interoperability among payers, providers, patients/members, and other interested parties who need health data. It is a one stop interoperability resource. The DGC primarily focuses on three areas:

1. Collaboration: Development of common understanding of and specifications for data standards, exchange mechanisms, and what it means to participate in the modern health IT ecosystem
2. Education: helping members understand their regulatory obligations, the data and exchange standards they're expected to use, and modern technology and related processes
3. Innovation: Identification and development of projects and services needed to make modern health data practices and exchange a reality

General Comments

This section comments on the general approach taken by CMS in their posted proposal or comments on items that cross multiple sections of the proposed rule.

Requirement to continue using HIPAA mandated X12 278 for Prior Authorization

We understand the use of X12 278 transactions for prior authorization is mandated by the current HIPAA transaction rules. However, these rules may be updated and, in theory, HIPAA has already made adjustments to accommodate portions of the May 2020 Interoperability rule. We believe such an update to permit direct FHIR API exchange for those who wish to use it in conjunction with this rule is warranted. At the same time, we recognize that not everyone is ready for this type of exchange and support continuing to allow for translation from FHIR to X12 as an option, at least for now, with a glidepath to FHIR support later. Having said that, we

also recognize that current adoption of X12 278 transactions is low, offering an opportunity to skip directly to FHIR only solutions for those not already supporting it. Thus, we also suggest recommending or perhaps outright requiring the FHIR only model for those not already using X12 278 transactions.

When discussing FHIR-centric prior authorization process with DGC participants, MHDC members, and others, this is frequently the first comment we hear. Having to arbitrarily map from FHIR to X12, potentially in both directions, for no reason other than to comply with existing regulations feels wrong to many people (including us). In addition to serving no purpose beyond compliance, it's onerous, adds to the burden using an automated prior authorization process is meant to reduce, and increases the possibility of introducing error to the process.

When addressed with CMS directly via questions in webinars or other venues, the response has universally been to use the exceptions process to get permission to skip this mapping and conversion step. This is not a viable solution for several reasons:

1. It's temporary. Exceptions are in place for no more than three years
2. It's onerous. The reporting and documentation requirements are extreme
3. It's expensive and potentially wasteful. Because of the temporary nature of the exception, organizations would have to divert money, personnel, and other resources to developing the FHIR-only process knowing they'd likely have to abandon the process without recouping the benefit of those expenses on an ongoing basis; further, they'd still have to expend the resources necessary to implement the regular process once the exception ends (or simultaneously if they are not using the exception with all of their partners or do not want to have latency between the end of the exception period and resumption of regular business without it).

We respectfully ask CMS to work with NCVHS, OCR, and other agencies within HHS as needed to change the X12 requirement in HIPAA before this rule becomes effective so it can be implemented directly as a FHIR-only exchange.

Approach to FHIR Implementation Guides

We believe that specific FHIR Implementation Guides should be required rather than recommended in most cases. Most of these guides have been around for several years now. Most have been tested in multiple connectathons, pilot projects, and in production environments.

Having consistent, well understood data fields with clear meaning that everyone uses the same way is a key element of any API or any successful data exchange. It is our view that most FHIR IGs do not go far enough in this respect, leaving too much about each defined field/property open for interpretation or variation. However, using standard IGs at least moves everyone into the same ballpark and gets them thinking about the need for consistency and standardization across exchange partners.

By merely recommending but not requiring the use of specific IGs throughout this rule, each implementation site is free to make their own choices about how to send data and how to represent the required data elements. It means that a provider interested in getting data through the Provider Access APIs from five or six different payers may have to use five or six completely different ways to log patient attribution and five or six different ways to accept the incoming FHIR data for patients associated with each of those payers. A payer looking to attest that they have a patient's permission to obtain data from a former payer has to do so by whatever different mechanism each of the payers with past relationships with their current patients outlines. And so on. Burden reduction from having a single way – or at least a mostly the same way with slight variations – to do anything mandated by the rule is lost because there is no single (or mostly the same) way.

We understand that one concern CMS has about requiring the use of specific implementation guides is that new versions of IGs are developed and they may be better or more efficient at mandated exchanges than current versions. While we have some concerns about this process as outlined by CMS, we point out that CMS has specifically built in a mechanism to advance versions of standards into this rule; there is no reason it could not be used for any or all IGs used to support these APIs or related auxiliary processes (patient attribution, etc.).

Version Advancement

We understand that it is not tenable or desirable to have people continue using older versions of standards for extended periods of time and, given the timeframe for implementation outlined in this rule, any or all of the related standards might be out of date by the time the rule becomes effective. We understand that releasing new rules solely to advance version is onerous and further delays adoption. We believe that healthcare as an industry moves too slowly and needs to be more agile and adopt development processes more closely aligned to those used in most other industries. All of that said, we have some concerns about the current process outlined for version advancement (we have similar concerns with the ONC SVAP process as well).

We believe consistency is key to successful data exchange. We consistently hear from DGC participants that the single biggest burden of their current data exchanges for quality measures, risk adjustment, and other purposes is that they are all slightly different even though 90% of the data needed for each department and each trading partner is the same data. We do not want to recreate this problem with FHIR.

This problem is exacerbated by the lack of backwards compatibility requirements in FHIR and most FHIR implementation guides. We believe that this is the crux of the problem and that a move toward more regular updates and backwards compatibility requirements that are standard features of APIs in every other industry would be extremely helpful and solve a lot of these problems. However, imposing such backwards compatibility requirements are outside of the purview of CMS and thus not a solution you can mandate.

Given the current state of the industry, allowing payers or providers and their various health IT to support their choice of several versions of any standard, be it implementation guide or other, is problematic. Inconsistencies, variation, and potential incompatibilities are more likely to be introduced to the exchanges. This increases burden, makes APIs less useful, and makes adoption both harder and less likely to happen in a timely manner without significant consequences for non-compliance.

Medication requirements for prior authorization and prior authorization data

We understand that there are NCPDP mechanisms for handling prior authorizations for medications, but having those processes completely separate and apart from other prior authorizations is problematic for several reasons:

1. Any tools, dashboards, or other software built to manage the prior authorization process within a provider organization must now support multiple mechanisms/processes for requesting prior authorization, gathering the required supporting documentation, submitting requests, reviewing responses, appealing denied prior authorizations, and other related tasks
2. The patient data as available through the Patient Access API would not include medication-related prior authorizations. Some patients will not understand why some but not all of their prior authorization data is available via this mechanism, and those that do will likely find the separation artificial and annoying.

Further, for many patients, these are the most common PAs they encounter and finding out their status can be more difficult than other requests as they involve more people and organizations (pharmacists/pharmacy staff, pharmacy benefit managers, payers, prescribing provider, etc) and everyone tends to point to one of the other actors as the correct place to get an update, or the information is only available piecemeal or not at all (the pharmacy may know that a medication needs a prior authorization, the provider may know one was requested, the payer may not yet have any information, the pharmacy benefit manager isn't willing to talk to the patient, etc)

3. The patient data as available through the Provider Access API would not include medication-related prior authorization information. Providers will not be able to see recommended treatments from other providers that have not yet come to fruition and may choose incompatible treatments of their own in the interim.
4. The patient data as available through the Payer=>Payer API would not include medication-related prior authorization information, potentially impacting continuity of care for these items. At best, the medication would appear in a medication list that was transferred, but none of the supporting data

needed to start a new prior authorization process at the new payer would likely be gathered together via the previous payer's prior authorization support data. While some or all of it may be included in other portions of the API exchange, collating that data is an extra burden/delay on the new payer. Further, should any continuity of care clauses be placed on existing approved prior authorizations, there would be no way to know whether there are any qualifying medications/what they are.

Further, it is our understanding that there are medications that are not covered by the NCPDP rules, such as infusions. In some cases, the medication and the delivery device are one and the same, meaning that there may be a medication and a medical device tied together under the same prescription/order/item. If they are not included in this rule, they will not be covered anywhere.

While we favor a single mechanism for all prior authorization requests, we realize that may not be possible given existing regulations and standards involving NCPDP processes. If this is the case, we believe it would be reasonable to still require all of the relevant data to be included in the Patient Access API, Provider Access API, and Payer=>Payer API. We understand this may require a new pathway for sending this information to the payer if they are not directly involved in making the coverage decisions but believe that it is the only way to make this process viable for patients and their ongoing care.

When this topic was discussed at a recent member interoperability forum, both industry experts and MHDC members attending the session indicated they felt it important for patients that prior authorization related to medications be included in this rule.

Coordination of Rules

There are a variety of currently proposed, pending, or expected rules from CMS that are not completely independent from each other; in some cases there may be components of different rules that contradict each other and in other cases they may be written in ways that unnecessarily increase the burden on one or more parties subject to the rule. These rules should be coordinated so that their requirements are compatible and executable without placing additional burden on individuals or organizations that need to implement more than one rule. None of these rules are implemented in a vacuum.

For example, look at this rule and the currently proposed attachment rule, Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard (CMS-0053-P). The attachment rule indicates that attachments used to provide supplemental or supporting information for a prior authorization should be sent using X12 275 transactions with C-CDA data. However, all of that data is required to be FHIR-ready for inclusion in the Patient Access API, Provider Access API, and Payer=>Payer API according to this rule ("The documentation required to be shared includes any materials that the provider sends to the payer to support a decision, for example, structured or unstructured clinical data including laboratory results, scores or assessments, past medications or procedures, progress notes, or diagnostic reports."). By not allowing that data to be sent from the provider to the payer in FHIR even if the provider is willing and able to use FHIR, an additional burden is placed on the payer to convert that data to FHIR resources that can be consumed by the Patient Access API, Provider Access API, and Payer=>Payer API.

This is just one illustrative example; we ask that CMS include a review for compatibility as part of all pending, proposed, and upcoming regulation to ensure that they are consistent and compatible with each other.

Prior authorization data retention time frame

While we agree that there is limited utility for the bulk of the support data and a history of use of approved prior authorizations with multiple visits/items/etc, there is some benefit to patients and providers to have a basic history of denied prior authorization requests. We propose that a simple list of denied prior authorization requests including the identity of the item or service and the date it was denied be retained indefinitely, in keeping with other data requirements for the Patient Access API, Provider Access API, and Payer=>Payer API. There are several reasons for this:

1. Patients may be asked what treatments were attempted for a particular condition or symptom by other providers or whether/why they didn't try a specific treatment. Having a list of previously denied prior

authorization requests can help them provide information about having not tried a treatment that they are not likely to remember (since they never had the treatment) and that might not be reflected in other available data such as encounters, procedures, medications, etc (since they didn't actually have the treatment).

2. Similarly, patients may be asked why they altered a treatment that had been working for them; one common reason for this is denial of a newly required prior authorization; being able to show that they took a medication or had physical therapy from time A to time B then stopped because further treatment was denied is useful

In addition, we believe that any data received as part of the prior authorization determination process that would fall under the previous requirements of Patient Access API inclusion (for example, belonging to USCDI v1) should be retained and exchanged in the Patient Access API, Provider Access API, and Payer=>Payer API outside of the prior authorization requirements along with all other such data obtained by the payer according to the rules of those APIs. We believe this is already mandated by the definitions of those APIs, but calling it out explicitly within this context would be helpful.

Assuring equitable access to patient data

One perhaps unexpected aspect of the current patient data access mechanisms already in place from prior regulations is that many payers (and providers) are requiring patients to both have a portal account and be able to access/log in to it to authenticate themselves for Patient Access APIs (or similar APIs from provider systems). Early discussion is already leaning toward similar requirements for requesting a new payer get data from an old payer using Payer=>Payer APIs and for other actions covered in this rule requiring some form of patient authentication, verification, or consent.

While this solution is fine for the 80%, it is problematic for certain elements of the population. For example, individuals with visual impairments often have difficulty or find it impossible to use provider or payer portals. These individuals might be able to access applications on a computer or mobile device if they had an alternate way to prove their identity, authenticate, or perform similar tasks currently requiring portal access.

We strongly recommend that alternate methods, perhaps centralized identity services, be proposed as a required alternative to portal usage for everyone to accommodate those who cannot – or would prefer not to – have a portal account they cannot or do not use.

Education about privacy and security of third party apps

While we agree patient education about the privacy policies and security of the third party apps they use is important, we also do not feel that providing such education should significantly delay their ability to connect to a payer with the app of their choice. We see the possibility of a payer causing significant delay by continued education if they do not like a particular app that a patient wants to use in hopes that the patient will give up and choose something else. We propose a time limit be placed on how long a payer can try to educate a patient about an app they want to use before they are required to allow the patient to start using it. We believe this should be a short timeframe, perhaps as short as one day. Alternately, a limit of the number of engagements with the patient might serve the same purpose. Placing a limit of a single interaction educating the patient about issues a payer might have with an app they'd like to use, or perhaps a single interaction followed by one follow up communication might serve the same purpose (so long as that follow up communication is not significantly delayed).

Third party apps from non-profit entities

We note that there is a hole in the current oversight of third party apps in that the FTC does not have any authority to provide oversight of non-profit entities. Thus, any third party apps created/owned by non-profits are not under either CMS/HHS or FTC jurisdiction. We do not have a solution to this issue, but felt it worth pointing out given your binary presentation of oversight (either HIPAA or FTC) within the rule text.

Detailed API specification

We believe the eventual goal of all healthcare APIs should be an explicit, specific definition of standard APIs

including exact, consistent definition of data elements (properties) and allowed/supported API calls/related API behavior (down to supported response codes, error states, etc). However, we understand the healthcare industry is not yet at a point where this is feasible. Given the resistance to even requiring specific implementation guides, which currently are high level specifications that do not require the level of standardization and consistency most APIs in other industries require, we do not feel this type of more detailed technical specification is possible – but it should be considered and kept in mind as a desired end goal as this and other upcoming regulations are written.

Further, while we understand this is not entirely under the control of CMS, we believe more specificity, particularly around what data elements mean, should be a goal of IG development to help move the industry in this direction at the fastest pace supportable. We also believe CMS could play a role in encouraging this with respect to ONC standards it uses such as USCDI and the resulting analogous US Core IGs.

In the interim, we feel the suggestions under Technical Documentation and other Implementation requirements below are a reasonable step that provides the information needed for implementation of APIs that are somewhat variable from user to user.

Technical Documentation and other Implementation Requirements

We note that this rule includes non-technical documentation and information dissemination requirements but does not include any requirements to create and supply technical documentation to those looking to use one of the APIs to connect to a specific payer. This is an oversight we believe CMS should correct. These should be part of every API – APIs are products and should include all of the same SDLC features and requirements as any other software product – but we know this has been a particular issue for the existing Patient Access API.

We have frequently heard feedback from third party apps trying to implement the existing Patient Access API that this is a significant barrier. Even when using the same implementation guide – something not required by this rule – there are implementation differences from payer to payer and these are almost universally not communicated to developers needing the information. The missing information range from the very basic (where to find a payer's FHIR server, for example) to how they handle the authentication and identity requirements to specifically what data they include in each property of the FHIR resources used in their version of the exchange (which, again, can vary greatly from implementation to implementation even if they're using the same IGs – what, exactly, does language mean in the sending system? What is the expected format for a patient ID? Is there a character limit to certain fields and, if so, is data truncated or is something else done if it's too long to fit? etc.) to many other details specific to each particular implementation.

In addition to a lack of API reference, API usage, and other relevant documentation, also exacerbating these differences is a lack of test data, staging environments, sandboxes, or other mechanisms to help developers test that they are getting and processing data sent via these APIs correctly.

A monitored mechanism for contacting a payer about implementation issues or with implementation questions is also an important missing piece to make widespread implementation viable. Again, looking at the experience with the existing Patient Access APIs, third party apps struggle with finding someone to fix issues, answer questions, approve their registrations, and address other barriers to implementation. Some have resorted to calling out payers on Twitter or other public arenas in hopes that it will get the attention of someone who can help with whatever they need (see [@JenBlumenthal](#) of OneRecord on Twitter for an example; although most of her recent tweets at the time of this writing are calling out providers and their EHR vendors, she has done the same for many payer organizations in the past).

Consistent rules about how to send OAuth tokens (for instance, requiring use of a specific header by everyone) and similar requirements that are part of every API call but that could be implemented differently by different implementations without further specification would also go a long way toward increasing API adoption, reducing the effort needed to implement them, and making them more useful to patients, providers, payers, and everyone else in the health data ecosystem.

Data Provenance

One concern we hear repeatedly from payers about all of these API exchanges is concern about presenting

data they did not directly generate to patients, providers, and other payers as if it was their own (we heard this about both the original Patient Access APIs and about all of the currently proposed APIs). We also believe in logging and data trails in general. Thus, we propose that all of these APIs support optional provenance resources that could be added by either the sending or the receiving entity to indicate the source of data if desired. Payers could use them to note when data originated from a provider or another payer if it makes them more comfortable presenting the data to the patient. These resources should be chainable, supporting the full history of the data from creation to present time. In addition to being able to note that the sender of data did not create it, this allows for a chain of custody for tracking down errors or determining the original provider of a piece of worrisome data to allow additional follow up if needed. We believe a standard provenance format should be defined for this purpose.

Standardized Prior Authorization Requirements for a Subset of Services

We believe that one way to greatly improve this process, decrease burden, increase standardization and consistency, and generally make things better is to select a subset of common services requiring prior authorization and defining standardized guidelines that everyone uses. Obviously there would be some services outside of this process, but there are many services with well defined and generally agreed upon clinical guidelines/real world evidence support usage that could be leveraged to develop a set of standard prior authorization rules, Questionnaire and QuestionnaireResponse resources, and other supporting components that would take the some of the burden out of the process. These services could be used to stand up prototypes and initial connections as payers develop the FHIR support for their other prior authorization guidelines/rules, would provide consistency to providers regarding whether prior authorization is needed and what's needed for approval, and give payers a head start in supporting the information used to make prior authorization decisions into the various APIs (see next comment).

We strongly believe this is the correct approach; participants in our Data Governance Collaborative agree. Further, we think it likely that such guidelines, if evidence-based and developed in a reasonable fashion, would likely be adopted beyond the required plans and perhaps make it more likely that payers would optionally support at least portions of this rule for plans that they're not required to do so.

Information Used to Make Prior Authorization Decisions

One of the requirements of the Patient Access API, Provider Access API, and Payer=>Payer API is inclusion of all information used to make the prior authorization decisions. We approve of this in theory, but have some specific concerns and suggestions related to how to do this in practice.

First of all, we would like to see some additional definition and standards around this data. We were left with many questions in this area, as were participants in our Data Governance Collaborative. Does it only apply to data sent directly by the initiating provider in support of the prior authorization request or is other data already known by the payer – either through claims or previous clinical data exchange – also part of the requirement? If information is sent by a provider to support a prior authorization request but the payer doesn't actually use it for that purpose, does it need to be included?

Given that the affected APIs are all FHIR APIs, the assumption is that all of this information needs to be sent via FHIR. However, there is no expectation or requirement that it fall within the US Core/USCDI clinical data sphere. Is the payer expected to define their own FHIR resources or profiles to accommodate this data? That would mean each payer would define these resources/profiles however they see fit and no standardization would exist. That would make the data difficult to absorb by providers, other payers, patients, and third party app developers. There needs to be a process for sending this data that doesn't devolve into having 9000 different resources or profiles that convey almost the same but not quite identical data.

While a group like the DaVinci PDEX workgroup could perhaps develop some standards for commonly expected types of data to help with this issue, there would always be data that doesn't fit that still meets the requirement of data required to be part of the APIs.

We again suggest that having some commonly defined prior authorization guidelines with accompanying standardized questionnaires and responses would also be of benefit here. In addition to defining standard Questionnaire and QuestionnaireResponse resources for these services, standard resources for the acquired

data as well as mappings from the response to those storage resources could help immensely.

We also respectfully suggest that FHIR support for attachments would be helpful here as well. We note that the current proposed attachment rule requires the use of X12 275 transactions with C-CDA data. While there is some ability to include some FHIR-formatted data within the C-CDA documents, being able to send entirely FHIR formatted data (preferably via FHIR APIs if the exchange partners can support it) for prior authorization-related attachments would enable payers to use that data as is without any unpacking, reformatting, or mapping in subsequent API exchanges rather than requiring payers to convert it from C-CDA to FHIR (and possibly to move it from their traditional X12 intake mechanisms and data stores to a FHIR warehouse or adding additional nodes to a FHIR façade). Taken as a pair, the attachment requirement adds an additional payer burden to this rule to map and convert additional data to FHIR. Given that payers willing to support FHIR for the actual PAS exchange are already constrained to make an extraneous FHIR ↔ X12 mapping (probably in both directions) for no reason beyond regulatory compliance, adding this additional mapping requirement seems especially burdensome.

Gold Carding

As there is no specific request for general comments about gold carding or the CMS approach to it within the prior authorization section of the rule, we will comment here.

We are not, in general, fans of gold carding without some form of extensive reporting and analysis component to track its effectiveness. There is too much potential for capricious action, or the appearance of such and we have heard many stories of the process turning contentious or disagreements around enrollment and disenrollment criteria for gold carding programs. There should be clear rules for both the issuance of gold cards and their revocation to limit these types of disagreements as much as possible if gold cards are supported.

Our Data Governance Collaborative participants note that gold carding eliminates data collection, standardization, and transparency – all goals that should be paramount when considering data-driven programs.

There was also concern that gold carding tends to favor larger, major provider organizations and thus may be an equity issue – patients at community health centers, private practices, and other smaller organizations are less likely to benefit from gold carding programs, setting up a system where patients at large academic medical centers or major regional hospital hubs do not have to deal with the burden, delay, and aggravation of the prior authorization process while those getting care within their local communities have to jump through these extra hoops to get the same care. Patients from disadvantaged groups tend to use these smaller options at higher rates than other patients, meaning they are more likely to be subjected to prior authorization requirements than other patients when gold carding programs are in use.

We were surprised to see the inclusion of gold carding in this rule, but, if retained, we believe some general guidelines for how to implement gold carding in a standardized way would go a long way toward avoiding some of the issues we've seen with these programs in the past. We strongly recommend CMS propose some specific rules around how to implement gold carding if desired that can be consistently and fairly applied to all who wish to use such a program. If possible, we recommend this be done in such a way that permits minor adjustments without additional rulemaking. Perhaps this could be done by defining the rules as a gold carding standard that could then be updated using the versioning process.

We understand that one of the benefits of gold carding is reducing burden and having extensive reporting requirements mitigates this, but we believe reporting about how the program is working is necessary and would help with adjustments and refinements to the program. We do not have a sense of specifically what metrics would be useful beyond some type of limited comparison of a subset of services rendered under gold carding vs whether they would have been approved by the payer's prior authorization rules for the same service. Perhaps a check of 5-10% of the rendered services for X number of services covered by the gold carding program randomly selected from among the covered services would be appropriate.

We also would like to see some reporting on the type of provider organizations qualifying for gold carding, their geographic locations/main service areas, and patient populations to help track the potential equity issues

outlined above.

Patient Experience and Patient Safety

We have seen a tendency in industry discussions about this proposed rule to focus on implementation efforts and the impact on healthcare organizations from a standpoint of time, resources, workflows, and personnel. Without disregarding that there are legitimate concerns in these areas, we urge CMS to prioritize the interests of patients in their thinking, particularly as so many of the organizations discussing and likely commenting on this rule may be more focused on the mechanics of implementing the rule.

Further, some of our DGC participants note that this isn't just a patient experience concern, but also a patient safety issue. Delays in processing prior authorization requests or denials without clear information about how to fix the request so it meets payer standards delays care, sometimes dangerously so.

Specific comments include:

- The stated maximum timeframes, while shorter than current limits, are still too long. There is no reason why a 24 hour timeframe could not be imposed on most if not all requests, with an expectation that more and more requests be handled in an automated and thus nearly instantaneous fashion as tooling and processes get refined over time.
- The denial reasons should include enough information to clearly indicate the reason for the denial with specifics and direct information about what is missing or needs to be fixed in order to meet the payer requirements or, if the case, that it is not possible for the patient to meet the requirements for approval. Both the patient and their clinician should have clear next steps to help them understand how to proceed and whether it makes sense to continue seeking prior authorization or look for alternate treatment options. It is not clear that the current X12 denial reasons meet this threshold (see further comments on this below).
- As noted above, the inclusion of prior authorization for medications is important to ensure a consistent patient experience. Most patients are not aware of the intricacies of the use of PBMs, separate NCPDP rules, or any of the industry insider reasons why support for medications is more difficult. They just know that medications - one of their most common interactions with the health system - are not showing up in their prior authorization information and that's a problem.

In short, regardless of thoughts on the specific suggestions above, we urge CMS to prioritize patients as they review comments to this proposed rule given many responses are likely coming from payer and/or provider perspectives and the patient-centric view may be less visible during the comment review process.

Response to Specific Questions – Patient Access API

This section will list specific questions asked about the Patient Access API in the proposal and our responses to them.

We request comments on how we can help give patients the tools they need to understand the privacy and security implications of using a health app within the scope of our regulatory authority.

We believe that one avenue that might be effective is the use of public service advertisements (PSAs) on television and in various online settings (social media sites, popular mobile apps, etc). We have seen PSAs for other recent regulations including the right to request your data via mobile apps (infrequently right after the Patient Access API enforcement period started) and for price transparency requirements and they seem informative.

Other avenues that might be effective include outreach from community health workers who might be helping patients with their care or programs that provide grants to FQHC and other hospitals and provider organizations to help them provide direct education to certain cohorts of patients likely to be high consumers of healthcare and thus likely to have lots of data to manage on how various federal laws and regulations impact

them and their privacy (for example, this could be part of diabetes care management programs, cardiac care programs, etc). This could also cover HIPAA as many patients do not understand their HIPAA rights or that HIPAA permits exchange of data without their explicit consent in certain circumstances.

Should there be a process at the time a developer registers an app with a payer for access to the API to submit information about its privacy policy? Should payers be required to provide that information in an easy-to-understand format the first time a patient requests access via an app?

We do not believe a delay to permit payers to absorb the privacy policy of each app a patient wants to use is warranted, and believe it would place a significant burden on payers who would need to hire additional staff to process, evaluate, and write easier to read versions of each app's privacy policy. Further, there is no guarantee more than one patient will ever want to use any specific app, particularly if the app is a specialty app meant to provide a very specific single feature or related to a specific type of care that isn't common.

Should payers notify patients, the first time the patients request data through an app, whether the app utilizes the MPN or not? Should payers be required to list apps that have established access to their API on their websites that comply with the MPN's transparency requirements?

We do not believe most patients will be familiar with the MPN and thus, if the goal is to help patients understand the privacy policies of the apps they use, telling them it follows the MPN rules will not be helpful. Further, it could be confusing as it is clearly something someone expects them to understand and they may not be comfortable asking questions or for clarification of what that means.

We also feel that there are other valid privacy codes that would give app users some comfort that the app takes privacy seriously. One such example is the CARIN code of conduct, an agreement mentioned by CMS earlier in this rule. We do not feel it appropriate to give precedence to one over another unless compliance with one particular model is being mandated (which is not the case). It is not reasonable to list all possible reasonable privacy codes to follow and thus it our feeling that none should be listed or given preferential treatment.

If a payer does have a preference for a particular privacy code/model, it is perfectly reasonable for them to mention that preference in their educational materials and why they feel that particular privacy code/model is one worth following or is preferred over others. Similarly, they could list apps they feel have particularly good privacy policies so long as they don't give them preferential treatment when it comes to supporting patients using them vs other options.

Can we leverage and build on other HHS health information exchange initiatives, such as TEFCA, to address these issues.

It is reasonable to expect apps to highlight their TEFCA compliance if they have it, and educational materials could help explain what that means in terms of privacy and security behaviors. However, since payers cannot give preferential treatment or refuse access to apps that do not comply, that seems likely as far as it can go.

We request comment on whether CMS should explore requirements or ways to encourage exchange under TEFCA as a way to ensure that more patients are informed about the privacy and security implications of using health apps to access their health information

Respectfully, we believe TEFCA is a step backwards in terms of app access at this time, particularly for data originating with a payer.

TEFCA as currently constituted is not a FHIR-based exchange. It is built on C-CDA document exchange - It does not provide a mechanism for receiving consistently structured data at a granular level (FHIR is not perfect at this either, but it is at least based on a structured data concept that attempts to define specific individual

properties for individually defined data elements) nor does it easily or automatically translate to FHIR.

Further, at the current time, TEFCA is more directly oriented toward provider=>provider data exchange than other exchanges and is not likely to provide the same type or quality of data potentially available via a Patient Access API if it's implemented correctly.

We understand that TEFCA has a roadmap for FHIR support and perhaps once that roadmap is executed this issue could be revisited.

We request comment on any actions that we can take to ensure patients' equitable access to their health information.

Please see the comment labeled "Assuring equitable access to patient data" above.

We request comment on what other Patient Access API metrics we should consider requiring payers to report to CMS and/or make available to the public on their own websites

We would like to see reporting on some or all of the following:

- Which FHIR resources are being requested through the Patient Access API, perhaps by frequency/number
- How many apps request all available patient data versus specific types of patient data
- The percentage of API calls that are successful vs unsuccessful and the list/type of errors returned (perhaps by percentage/frequency)
- A list of apps patients use
- A list of apps used by more than X patients, where X is one or more specific numbers TBD

We are seeking comments on whether payers could report aggregated demographic information, such as sex, race, age, ethnicity, and geographical (for instance, by zip code) data

We believe all of the data listed above would be useful, as well as information about disability (by type if available).

Response to Specific Questions – Provider Access API

This section will list specific questions asked about the Provider Access API in the proposal and our responses to them

We request public comment on the proposal for impacted payers to implement and maintain a Provider Access API to provide access to specified patient information.

We believe that out-of-network providers should be able to access the Provider Access API so long as they can meet the requirements for showing they have a treatment relationship with a patient. This standard should be the same for all providers, regardless of network status.

We also believe that the standard of patient relationship should not hinge on a patient having a single appointment on the books with a provider, particularly given that this API is set to opt out rather than opt in. In particular, we are concerned about the ability of patients to get independent second opinions if their second provider has full access to all of the data, treatment notes, comments, opinions, diagnoses, and other data from the original provider. This information will bias the second provider even if they make an attempt at independent evaluation (which not every such provider will do). Another concern with a standard of a single

appointment is that the patient and provider do not know if this will be an ongoing relationship or a one time appointment. In the latter case, there is no need for the provider to have access to the patient's data and, in some circumstances – such as the patient choosing not to return because of an issue or problem with the provider – it would be inappropriate for patient data to be maintained by that provider.

Given that the patient does not have to opt in to this API, we favor some type of model whereby the patient identifies the providers they consider “their providers” – i.e. those providers with a treatment relationship with the patient. Some form of trigger or inquiry could optionally be sent when a new provider is seen, if desired. If this is deemed too onerous or difficult to maintain, we believe a second appointment with the same provider – not the same office, but the same individual clinician – would be a reasonable trigger to indicate a treatment relationship exists. In the interim, the provider could acquire any data specific to the first visit either by virtue of being the ordering clinician, via direct patient request that the data be shared (patient consent form, etc), or by the patient directly sharing data they've acquired through other means (Patient Access API, patient portals, health record requests, etc). Once a formal treatment relationship has been established, direct electronic versions of any data acquired via other means would flow and backfill the electronic records at the provider.

Another option would be to open the formal patient attribution mechanism to out of network providers, allowing providers to send payers verified patient lists of the patients they treat. We propose that a second visit still be the threshold for this mechanism (we considered the idea of scheduling a second visit rather than having one, but many providers schedule appointments without patient permission or knowledge with the expectation that the patient can change or cancel it if they wish so having a second appointment scheduled does not convey patient intent to have an ongoing relationship).

We understand there may be cases where a patient wants a new clinician to have a treatment relationship in place immediately and get all of their data ahead of time; this is part of why we favor the “patient identifies who they have a treatment relationship” model. However, when the patient wishes are unknown, we believe in erring on the side of not sharing, per the reasoning outlined above. Once seen, the data cannot be unseen.

As a corollary, we believe it is essential to have a clear mechanism for severing the treatment relationship with a provider. Our Data Governance Collaborative participants agree that this is a necessary component of the rule. Again, ideally this would be patient-driven – patients should have the ability to sever a specific relationship at any time (an alternative to this would be a more granular opt-out process allowing the patient to opt out of sending data to just that provider).. We also believe that a timeout process whereby if a provider isn't seen within a certain length of time – perhaps 2 or 3 years – the treatment relationship is either automatically severed or, if possible, the payer sends an inquiry to the patient asking if they are still seeing that provider. If they say yes the relationship is retained, no it is severed. While this would not remove data already acquired by the provider, it would prevent them from getting new data the patient doesn't want them to have.

As noted above, we believe a treatment relationship should be between a patient and a particular clinician, not an entire provider organization. We realize that data sharing among that organization may be automatic and this may be an artificial consideration from the standpoint of data access, but for the purposes of treatment relationship if a patient sees two different clinicians from the same office once each, that should not be considered two visits to the same provider if such counting is a consideration for determining if a treatment relationship exists.

Finally, our Data Governance Collaborative participants believe CMS should directly address the case where requests are coming from a third party, such as a vendor acting on behalf of a provider. How does a vendor show that they have permission to act on behalf of a provider? Can different components of the required information come from different sources – for example, can the provider supply patient opt out information while the vendor handles the actual API requests? Does the vendor need to be part of the provenance information (we vote yes to this)? Are there other considerations when a vendor is handling the provider data access and exchange?

We invite comments on whether we should establish more explicit requirements regarding patient opt out processes.

We believe there should be some common language that outlines exactly what opting out or opting back in

means for a patient. We also believe payers should be required to provide multiple mechanisms for opting out or opting back in including via portal, customer service phone, email, and perhaps via postal mail.

We request comments about the technical feasibility of implementing an opt out process that would allow patients to make provider-specific opt out decisions, and whether we should consider proposing such a requirement in future rulemaking.

While we cannot comment on technical specifics, we believe the ability to opt out of sharing with specific providers or provider offices is essential. An alternate mechanism for this is allowing patients to remove/sever the treatment relationship with a provider, thus removing their ability to receive data about the patient.

We request comments on our proposal for a patient opt out framework for the Provider Access API.

We believe opt in is a better option. We accept that technically HIPAA makes an opt-out model legal and that consent is technically not required as long as a treatment relationship exists. However, we believe patients should be at the center of the healthcare system and have control over their own data whenever possible.

Some of your stated justifications for deciding to switch to opt out seem a bit strange to us. For example, the statement “A report produced for ONC found that states using an opt out model were quantitatively associated with significantly higher HIE utilization” – there was more data in the system, therefore the system was used more. But that doesn’t address whether they should have had access to that data. Higher usage should not be the main end goal – the highest amount of appropriate usage should be. A data mining service that connects to someone’s email client might have access to more people’s contact information than it did before the connection, but that doesn’t mean it has the right to have or use that data, and it likely doesn’t - the increase in data in that case is bad, not good.

We also reject the argument that opt in is better because it ensures that people with health literacy deficits or who don’t speak English well or are otherwise disadvantaged will have their data shared. Assuming that someone cannot understand what it means to consent and therefore the system should consent for them is not the right approach; taking the time to explain those rights so anyone can understand them and giving them a choice is. To do otherwise is treating them as incapable or less than. Even if it’s true that a percentage of people do not fully understand what it means to exchange this data, we believe this makes it more important that the default protects their privacy. If they genuinely do not understand what consent is or what it means they should not be forced to consent by default.

We additionally request comments on whether patients should be able to exercise more granular controls over which data they permit the payer to share, including permitting the sharing of certain data from only specific timeframes

We are in favor of granular controls in general. Sending a specific type of data from a specific timeframe is a perfect example of the right way to send data to someone offering an independent second opinion (to return to that case). There are other use cases where it makes sense, and likely is also preferable to the receiving provider as well. For example, a physical therapist likely only wants data specific to a particular injury they’re treating – and a patient has no reason to want to send them anything more than that and may consider requests for more a red flag. If it turns out the provider needs additional data later during treatment, they can request it at that time with patient consent.

When using old-fashioned paper consent forms, patients almost always have the option to specify exactly which type of data from which timeframe associated with which provider is allowed to be sent. If the goal is to have patients participate in electronic exchange, giving them the same level of control seems obvious. Otherwise, patients wishing for that level of control will opt out of electronic data exchange and continue to use more burdensome, more manual processes that give them the control they want.

We request comments on whether there are benefits or burdens to requiring that

this information be provided in a specific format or to include specified content.

We believe there is some benefit to having some standards for educational materials related to the Provider Access API. We favor a model where some text is provided as guidelines as a starting point for everyone but that allows for some adjustments based on population characteristics. There should be some additional guidelines regarding which languages to provide (top 5 for the location, most requested translator services in the organization are two possible options) and a requirement that the text be available in large print, audio or video recordings, and perhaps in some other formats. Printed materials should use clean printouts (no photocopies) and materials should be available online (as already required by the rule). in a format that does not override user browser settings or otherwise interfere with a patient's ability to display the text in a form easiest for them to read.

We also request comment on whether providing this information at the time of enrollment and annually is appropriate, or whether we should require that this information be provided directly to the patient more frequently.

We suggest that any written communication include a link to a section of the payer's website that includes the required educational materials for each of the various APIs. While supplying information in annual forms sounds good in theory, in our experience many plan renewals do not actually generate patient-visible paperwork, forms, or formal documents of any sort. Even at initial enrollment time, it is often difficult to get much more than the actual enrollment forms from a payer and maybe a plan overview document. The main communication mechanisms between patient and payer are explanation of benefits notices (either paper or online or both). Thus, these should be leveraged if possible.

We request comment on this proposal, including whether CMS should develop guidance regarding, or address in future rulemaking the specific content of these educational materials about the Provider Access API.

We understand the need for some level of non-technical documentation to help everyone at a provider organization understand the need for APIs and the basic way they work, but per our general comment above, in order to actually facilitate implementation technical documentation is needed.

At the general level as outlined currently, we do think the following should be required in some form:

1. A list of implementation guides used as part of their specific implementation, including links to each formal IG in HTML format for online viewing. This should include any home grown IGs or IGs from local associations/organization/communities as well as IGs from national standards organizations.
2. A link to technical documentation to support implementers
3. An overview of their approach to the API to help users understand how best to interpret their data
4. An overview of their internal testing process at a high level (omitting any potential security risks)
5. A list of known bugs or issues with the API, updated on a regular cadence (perhaps monthly?)
6. A link to an application registration form or other mechanism to initiate registration for token generation
7. High level release notes or deltas between new versions if/when the API is updated and new versions released
8. An email address, web portal, and/or phone number for implementation assistance/basic questions not covered by documentation with a requirement that inquiries be monitored and a response process is initiated for non-spam requests within a certain amount of time (perhaps 2 business days)

We do not, at this time, suggest requiring specific content for each of these items.

We also recommend that similar documentation be required for the other mandated APIs.

Response to Specific Questions – Payer => Payer API

This section will list specific questions asked about the Payer => Payer API in the proposal and our responses to them

We request comments on these proposals (general request at end of overview)

We fully support the change to require Payer=>Payer data exchange use FHIR APIs. We also applaud the idea of supporting all requests whether or not the other payer is subject to this regulation, but we do have one concern regarding this from a practical standpoint:

If a patient's new payer is subject to this regulation but their old payer is not (for instance, if they are switching from an employer's commercial plan to a Medicare Advantage plan as they reach the age of 65), how is the new payer expected to send API requests to the old payer if they choose not to optionally support the Payer=>Payer API? The new payer needs an endpoint, authentication process, etc. at the old payer to send it API calls and those do not exist. Thus, from a practical standpoint, it is not possible for the new payer to comply with a CMS directive for "an impacted payer to request patient data from another payer...regardless of whether the other payer is an impacted payer (a status that may or may not be evident to the requesting payer)."

Instead, we propose a requirement that the new payer inquire whether the old payer supports the Payer=>Payer API as outlined in this regulation *and* request enough information to determine whether the old payer is supposed to support it. If they do not support it and are not required to support it, they can note that and perhaps report it as part of the reporting requirements. If they do not support it but clearly are supposed to support it, they should be required to submit a non-compliance notice to CMS. We recommend CMS include a simple process for doing this in the final rule – perhaps just a monitored email address and a few required pieces of information (payer name, plan name if known, why they think support should be required, date they were told it wasn't supported, name and contact info of the person who told them it wasn't supported if known). Some type of consequence for non-compliance should be levied if the reported payer is, indeed, supposed to be compliant but isn't.

We would also like to comment on the CMS expectation that having implemented one FHIR API with similar or the same data requirements, implementing more would be an easy lift for a payer organization. On its face, this statement feels objectively true. However, we have discovered this is not always the case. Payers, like many other organizations within the healthcare ecosystem, often suffer from a phenomenon we call process silos. These are essentially cases where the right hand doesn't know anything about what the left hand is doing. If one business unit, group of developers, or other subunit of a payer organization was responsible for implementing the original Patient Access API, other groups within the same payer responsible for other functions and activities may have no idea that any FHIR support was implemented at their organization at all. This seems ridiculous on its face, but we have found it often to be the case nonetheless.

We do not know what the solution is to breaking up these process silos beyond encouraging better communication at the top levels of organizations. In an ideal world they would not happen and we are not necessarily recommending CMS alter anything because they do. However, ignoring the realities of the current state of organizations will not help make barriers go away and we have found this phenomenon to be a barrier to increased FHIR adoption for any number of potential uses. We also note this comment is not specific to the Payer=>Payer API but since CMS specifically comments that they considered the similar requirements of other FHIR API requirements in their assessment of Payer=>Payer APIs we felt it appropriate to mention the issue here.

We are also interested in comments about whether the continuation of a prior authorization or additional data exchange could be particularly beneficial to patients with specific medical conditions.

We believe that a 90 day continuity of care clause, similar to the continuity of care clause included in the No Surprises Act when a provider moves from in network to out of network, would be appropriate for all patients.

We would welcome payers choosing to honor PAs from a previous payer for a longer time period, but 90 days would give the new payer time to evaluate information received via the Payer=>Payer API at enrollment, determine if additional information is needed to initiate and evaluate its own PA for the service, or determine a possible appropriate alternative if the service is one they normally do not cover (or start a process to cover the treatment anyway based on guidelines and coverage rules). Further, CMS has already established 90 days as a standard continuity of care window so this would just be applying existing standards to a new use case.

While we believe this should be required for all patients, we feel particularly strongly that it should be required under the following situations:

1. If the service is scheduled within 30 days of the start of the new coverage (we believe 30 days is the right number, but would argue 15 days should be an absolute minimum).
2. If the service is generally scheduled more than X days in advance and not honoring the existing PA would require rescheduling the service (we suggest picking an X somewhere in the 90-180 day range; we do not necessarily have a good feel for an exact number that makes sense but believe one should be chosen)
3. If the patient is disabled or has some other circumstance that makes it more difficult to perform the service or more likely that others are helping them acquire the service (including scheduling, transportation, or other service-adjacent aspects of the process)
4. If the patient has specific requirements around seeing a provider who speaks a certain language that restricts scheduling options
5. If the patient has cancer or another potentially aggressively progressive disease whereby delays could significantly adversely affect their health outcome
6. If delay would cause significant financial harm to the patient in some way

We believe this 90 day window should be required even if the new payer does not normally cover the service in question as finding alternate treatments takes time, particularly for patients who may have already tried other options that failed to help them, as does using payer processes to get coverage for items they normally would not cover if deemed the best course by the patient's providers.

We request comments for possible future rulemaking on whether prior authorizations from a previous payer should be honored by the new payer, and if so, should the prior authorizations be limited to a certain period of time based on the type of prior authorization or patient's medical condition? If so, what should that timeframe be? Should prior authorization from a previous payer be honored in certain instances regarding specific medical conditions? If so, which conditions and for what timeframe?

See above. We believe this should be part of the current rule, not delayed for future rulemaking. If a partial implementation is applied to this rule, we strongly support a more robust continuity of care provision in future rulemaking.

We request comments on which data elements would be necessary or extraneous to make that Payer-to-Payer API request.

We concur with the comment that patients should not be required to supply specific plan names to their new payer. Plan names are often long and use many unintuitive acronyms or abbreviations. There is often very little difference between the names of different plans offered by the same payer and those differences may be toward the end of the full plan name where they are likely to be truncated in certain communications. Further, some patients may have multiple plans over time with the same payer; remembering them all may be difficult and only supplying one might preclude obtaining data from others.

We propose a minimum standard of full patient name, date of birth, phone number, physical address (if one

exists), and payer name be required. We believe a patient should be encouraged to supply as much of the following as they can on an optional basis: date of coverage start, date of coverage end, and perhaps up to three recent services covered by the old plan with their dates of service as an additional verification mechanism (we are not certain whether this would be helpful or a hindrance given that the patient would likely use different terminology to describe these services than a medical professional would in at least some cases and certainly would be unlikely to provide codes that map to specific services recognized by the payer so this may have its own matching issues that would prevent otherwise valid matches from being successfully recognized).

We do not believe a group number should be required given that they are typically associated with a single plan as opposed to the patient's entire history with a payer. We are on the fence about requirements of a member ID and/or SSN both for the same reason (member ID is likely plan specific, and may or may not include the patient's SSN) as well as concerns about exchanging SSN information as an identifier for security reasons when the number itself is not needed for its legally designated purpose (financial transactions of various sorts and confirming identity related to such). At the same time, we recognize that patient matching is a challenging activity and that even names that seem less common may be used many times over within a specific payer. Finding the correct balance to ensure proper identity while maintaining an appropriate level of security is an art, not a science. However, we feel that SSN is among the most dangerous piece of data to exchange given the many avenues well beyond medical it opens up should it be compromised and its use should be limited as much as possible.

We request comments on our proposal for an opt in process for gathering patients' permission for payer to payer data exchange.

We strongly agree with using an opt in process for this API. We favor opt in generally, but this API is particularly well suited for an opt in process given that, unless concurrent payers are involved, it is a one time (or time limited) exchange. Further, as noted, it requires information from the patient to initiate.

Would additional data be helpful for the new payer for weeks or months after enrollment?

We suggest a requirement of a second, follow up exchange 30, 60, or 90 days after the initial request is fulfilled to capture any additional claims processing or clinical data sent to the payer during that timeframe. We suggest that this not be an ongoing exchange during this time window, but a single exchange at the deadline (or perhaps within 3 days after the deadline) to send all remaining data at once. This would reduce the burden of ongoing exchange and provide an expected cadence of when new data might become available. We believe this delay is likely acceptable given that time-sensitive data such as prior authorization requests were likely either completed or stopped in an incomplete state at the time the old coverage ended so this is mainly backfilling a minimal amount of claims, encounter, and clinical data filtering through the system.

We seek comment on whether the proposed timeframes for a new payer to request patient data, and for the previous and/or concurrent payer to send these data, are appropriate or whether other timeframes would better balance the benefits and burdens

We believe having one week to submit collected opt-in data is sufficient provided the patient has supplied sufficient data (if enrollment is only offered electronically we believe 3 days would be more appropriate, but paper enrollment is still supported by many payers so time for data entry is needed). We propose that the wording should perhaps be a one week deadline to initiate exchange if a minimal required set of data is available. Similarly, we believe the old payer deadline should be to respond to the request and acknowledge it's a valid request (i.e. verify the previous enrollment of the patient) and to supply the data if all of the necessary identifying data and consents are provided in the initial request.

In general, we believe APIs should be executed in real time. If the data is truly available in FHIR format as required for other APIs (and, in theory, already in place for all but the prior authorization data from the existing Patient Access API) this should be possible. However, given the propensity for process silos as outlined in a

comment above, we are not certain that having this same data available for Patient Access and Provider Access APIs necessarily means it will automatically be available for Payer=>Payer APIs.

Also, given the likelihood that more data is being requested for a patient in the Payer=>Payer exchange than for any single Patient Access API or Provider Access API (we anticipate most of those requests involve an initial request for data from January 1, 2016 to that current date followed by subsequent requests for only new or updated data since the last request whereas Payer=>Payer requests will entail sending all data at once) it may be reasonable to allow some amount of extra time to accommodate exchanging a larger body of data. We do not feel strongly about extending the timeframe to 3 days, but think it might be reasonable to do so (see reasons why it may not make sense below).

Further, given the patient is expecting all of their data to be in flux, delay of this API is likely more acceptable than delays in other CMS-mandated APIs. We do agree that prior authorization is more time sensitive than other data, so perhaps a requirement that PA data be sent first as soon as it's available might be a reasonable compromise position. In general, we think the data from this API could be sent on an "as ready" basis as opposed to all at once provided the receiving payer knows to anticipate its receipt that way.

That said, given that patients have variable amount of data, there is no reason to assume that one patient's entire medical record from January 1, 2016 will contain more or less data than even a small portion of a different patient's medical record, just that it contains more data than their own partial records. Thus, one could argue that if 1 day is sufficient for the other APIs for any patient it should be sufficient here, hence our lack of strong feelings about whether the required time frame should be 1 or 3 days. We do feel that if a longer time frame is offered for this API, 3 days is more than sufficient.

We request comment on these proposals.

We have heard general concern from payers that an attestation from another payer that a patient has given consent to this exchange is not sufficient proof of consent for their comfort. Perhaps a requirement that a FHIR consent resource be included with an initial Payer=>Payer API request should be considered. Alternately, some assignment of legal liability to the requesting payer might assuage these concerns (but may not be acceptable to the requesting payer as there could be liability around poor patient matching or for other reasons even when both sides act in good faith).

We note that one purpose of this exchange is meant to power the ongoing Patient Access and Provider Access APIs. This is obvious from several comments throughout the rule, both in explicit statements that a payer would no longer be required to support these APIs once coverage lapses and brief mentions that data should be incorporated into these other APIs as appropriate in order to maintain ongoing patient access to all of their data, such as if they get a new app and want all of their data from January 1, 2016 as is their right. CMS does explicitly state this, but we believe there are some additional requirements to consider. In particular, we believe data acquired via Payer=>Payer APIs should be dated with the original date of service to prevent its duplication should an existing app request only data from a specific date prior to the acquisition of the data from the old payer forward.

Finally, some payers are reluctant to present data they did not collect as originating from them. CMS mentions an optional ability to note this, but we propose creating specific provenance resources indicating the data came from the old payer on date X that could be optionally supported/included in subsequent data exchanges using that data, enabling this to be done in a standard way across all payers. See our general comment about data provenance for a more complete discussion of this idea.

We request comment on whether our understanding is correct and whether there is a benefit to us considering a data retention requirement in the future.

We believe that there should be a data retention requirement, particularly as some patients may move in and out of plans required to implement these APIs. Thus, if payers are not required to maintain data then the next time a patient is covered by an impacted plan chances are they will not be able to get their older data. Further, the option to opt in after enrollment is supported (and originally was intended to be the only option) and may be used by patients who require some additional education before being comfortable with this type of data exchange. We note that requiring patient education about opting in on an annual basis implies some

expectation that the ability to opt in still exists on each of those occasions and that the relevant data still exists at the patient's old payer. Otherwise sending documentation about how to opt in would be contraindicated.

If the intent truly is to maintain a longitudinal patient record starting from January 1, 2016 then data should be retained from that point forward. However, we realize this is a potential burden so we suggest CMS consider one or more of the following options:

1. Data retention of all data is required by an old payer until such time as another payer requests that data via the Payer=>Payer API. At that point, its custody is shifted to the new payer and the old payer has no further responsibility to maintain it (perhaps a short retention period past that point is warranted to ensure any errors or glitches can be corrected might still be warranted)
2. Data retention is required for X years (5 at a minimum but we prefer 10) after the relationship is severed. The old payer is required to attempt to notify the patient 1 year and X months (3? 6?) before the deletion date to let them know that their data will be deleted; please request it be sent to another payer by X date to regain access to it. A copy of the payer's educational materials about the API should be included with these notices.
3. Data may be archived after X years (perhaps 3?) but it can be restored and sent via Payer=>Payer APIs upon request with a 30 (60?) day delay for its retrieval and any required reformatting

Our Data Governance Collaborative participants note that data retention is helpful for calculating HEDIS and other quality measures and recommend that the longest quality measure timeframe be the minimum data retention length. We believe this is 10 years.

We request comment on whether it would reduce payers' burden to only be required to provide these materials annually to any patients who have not opted in and those with known concurrent payers.

We cannot comment on the burden, but we repeat an earlier comment that many patients do not get regular re-enrollment or other annual notices so if the intent is for patients to see this information a short notice with a link to the educational materials on the payer website on both paper and electronic explanation of benefits notices would be the most effective way to ensure the most patients actually have access to the information.

Response to Specific Questions – Prior Authorization Process

This section will list specific questions asked about the prior authorization process in the proposal and our responses to them

We request comments on this phased-in approach, our assumptions, and other potential options for an implementation strategy.

In general, given the time frames proposed for this rule and the likelihood of extensions or enforcement discretion extending those dates even further into the future, we do not favor a phased approach, in that we believe the entire PA process should be implemented within the next several years. Should a phased approach be taken, we believe a better approach is requiring support of the CRD functionality first, followed by the DTR functionality, followed by the PAS functionality rather than an approach that requires implementing the entire process for a portion of prior authorizations. There are several reasons for this:

1. There are direct patient benefits from having real time CRD support available during discussions with clinicians as they can adjust their treatment in real time based on prior authorization requirements should they deem it appropriate. Without this component, many encounters or conversations wind up being wasted time for both participants as they agree upon an approach that cannot be realized or realized within an appropriate timeframe when some of the time an equally appropriate treatment may be more accessible. In cases where it is not and a prior authorization is initiated, the patient and provider can discuss the implications of any delay and how to mitigate its effects if that's possible
2. If each payer implements 25% (or some other partial set) of their PA requirements and there are no

requirements for which services are implemented in each batch, providers would need to support the requirements of all of the PAs required by any payer. While most of the technical lift is likely absorbed by their EHR or other health IT, there is still a mental burden on clinicians who have varying information available for different patients depending on their payer.

We are likely to recommend this approach to payers regardless of the official CMS requirements, but with timelines that get payers to PAS implementation by the required January 1, 2026 date. In particular, Massachusetts is considering adoption of statewide requirements for CRD using the DaVinci implementation guide. This would be completely in line with this rule regardless of the implementation strategy either required or recommended by CMS.

If a percentage phased approach is taken, then we strongly suggest that the phases be standardized and certain types of services be assigned to each phase. This may still impact different payers and providers differently depending on their patient populations and the service they offer, but it would at least offer some level of predictability.

We also offer an alternative: we believe it would be beneficial to identify a group of common services and define standardized PA requirements for them that all impacted payers would use. We also suggest defining standard Questionnaire/QuestionnaireResponse resources for each of these services so everyone is collecting the same data to feed into those requests. If this approach is adopted, then we could see a phased approach where these common services are implemented first given that they will be a much smaller lift and end-to-end PA connections could be tested using these services. Then additional services defined by each payer could be implemented with a later implementation date requirement. This would provide predictability and give each pair of exchange partners a proof of concept with well defined, consistent services. The expectation would be that the technical lift for PA would be separated from the data/guideline definition and documentation requirements definition and could proceed in parallel, allowing the second stage to follow the initial stage without an extensive period between them.

We request comment on additional steps CMS could take to encourage providers and health IT developers to adopt the technology necessary to access payers' PARDD APIs.

We do believe some additional action by ONC around prior authorization is likely warranted. In particular, we proposed several support features certified health IT should be expected to support to help track the status of existing prior authorization requests holistically within a provider office. Having some dashboard and reporting tools available within EHRs or other certified technology would be extremely helpful to office staff used to using portals to manage prior authorizations. In addition, certifying SMART on FHIR apps that support the PARDD APIs and the related documentation gathering process would be extremely helpful. There was some discussion of ONC certification of payer technology related to prior authorizations; perhaps this is an area where CMS and ONC can act hand-in-hand to improve adoption and support.

We believe the biggest encouragement to adoption is including as much standardization and consistency to the process as possible. This is one reason why we oppose a phased approach allowing payers to select which services to implement first. We believe having some common services where the prior authorization guidelines are standardized across the industry as discussed above would be extremely helpful to this process as it gives additional consistency to providers and helps them better understand whether prior authorization requests are likely to be approved or not.

We request comment on the proposal to require implementation of a Prior Authorization Requirements, Documentation, and Decision API.

We are strongly in favor of requiring a PARDD API, but believe it should require use of the three DaVinci prior authorization implementation guides. We further believe that CMS should work with NCVHS, OCR, and other relevant organizations within HHS to alter the requirement to use X12 278 transactions for prior authorization. As noted, this standard is not currently widely used, meaning that folks will have to develop an implementation now just to be able to do a FHIR-based exchange they then have to convert to X12. It makes much more sense to just require the use of FHIR from the start for those organizations not already using it and to offer a

glidepath to FHIR for those that are. Please see our comment above in the general section for further thoughts on this matter.

Given that this rule does not require the use of the three DaVinci prior authorization implementation guides, the rule does not specify very many specific requirements for the API. This will lead to additional burden on all sides as each payer and provider will need to support multiple mechanisms for exchanging the required data in order to exchange with all required exchange partners per this rule.

Since there is no separate request for comment within the denial reason section of the proposed rule, we will comment on it here. We very strongly support the inclusion of denial reasons for every denied prior authorization request in both the PARDD API and the other relevant APIs. However, the reason codes supported by X12 are limiting both in terms of scope and in terms of the amount of detail they provide.

As stated several times, we support the removal of the X12 requirement, but as long as it remains we strongly recommend CMS work with X12, NCVHS, and other relevant organizations to expand the denial reasons and to add support for more verbose and specific options. We believe that these reasons should include sufficient information to fix the problem; this likely requires identifying specific missing properties within the collected FHIR resources, why certain included data is insufficient, or other reasons requiring specific comment about particular properties. It is not at all clear that, even if these could be called out in X12, there would be a useful way to convert these comments to the relevant FHIR data in such a way that FHIR APIs within an EHR, SMART on FHIR app, or other automated mechanism could understand and act on the reason. It is not even clear if enough data would be included in this reason code to guide a manual lookup of data without some external process to determine what else needs to be done.

We request comments from all stakeholders, including payers, providers, and consumers, on how the information might be displayed on payer websites in a useful and meaningful manner for patients and providers, including which data would be most useful.

We believe that having a standard reporting format would make comparisons across payers and/or plans much easier and also make specific data someone is interested in finding easier to find.

Further, some of our Data Governance Collaborative participants believe the most likely common use for these reports is absorption into third party apps that collate the data in various ways and compare different payers/plans to each other. Implementing these types of apps is extremely difficult without some type of consistent data and data format.

We request comments on the proposal for reporting metrics on prior authorization, for example, on the proposed types of data to be included in the report, on the proposal to report data in aggregate by items and services, on the proposed reporting timeframe, the number of reports, and if there are any other types of data that could be useful to payers, providers, and patients.

In addition to aggregated data across all items and services, we also would like to see specific data for particular common services, perhaps those with standardized guidelines should CMS adopt that idea. This would allow a direct comparison of like to like across different payers and plans. Certain prior authorization requests are more complex than others; if a particular population served by a plan or payer requests more of those services than the population served by a different plan or payer then comparing the decision times of the two is not a fair comparison.

On that note, some mechanism to measure the percentage of services requested or perhaps a list of the 10, 25, or 50 most commonly requested PAs for a particular plan or payer would be informative

Providing data for some or all of these metrics sliced by various demographic data such as race, ethnicity, disability, etc. might give some insight into the equitable application of prior authorizations.

We are not sure that requiring the first report on March 31 covering data prior to the implementation of the rule

necessarily makes sense, although having some baseline data on things like time to decision might be helpful.

Given that use of the PARDD API would develop over time, we also request comment on the timing for adding a metric similar to those proposed for the Patient Access API in section II.A, for the total number of prior authorization requests received via the PARDD API. This information could be useful for evaluating the degree to which API-facilitated requests would grow over time.

It was our expectation that CMS expected all prior authorization requests to use the PARDD API as of January 1, 2026, although obviously there is always some lag in compliance until some type of strict enforcement actions are implemented. Thus, while we see the benefit of measuring adoption over time because of practical considerations, we are concerned that this comment as written sets the wrong expectations and encourages a slow adoption. We also wonder if it represents some fundamental misunderstanding of CMS intent on our part which would be unfortunate. We ask that CMS carefully consider the language it uses in the final rule around adoption expectations and that there is consistent clarity in this area across every portion of the rule.

As far as the actual metrics, we suggest the following metrics be considered for adoption:

- Number of requests initiated using PARDD API
- Average response time for requests not requiring a prior authorization
- Number of requests initiated using PARDD API requiring a prior authorization
- Number of requests initiated using PARDD API requiring a PA that had all of the required documentation available automatically
- Percentage of PARDD requests requiring a PA with all required documentation available processed automatically without any manual intervention
- Number of requests initiated using PARDD API requiring a PA that were unable to automatically supply all required documentation
- A list of all SMART on FHIR app/EHR combinations or equivalent technology used for PARDD API requests at provider organizations

We seek comment for consideration for future rulemaking on how to measure whether and how such gold-carding or prior authorization exemption programs could reduce provider and payer burden, and improve services to patients.

We do not have any real ideas on how to measure whether gold carding is improving services to patients as that most likely would come through time savings that allow staff to spend time on other tasks; whether those tasks constitute improved services to patients is dependent on what those tasks are and likely is highly subjective. We did suggest a check of how a gold carding program tracks with the payer's normal prior authorization for a subset of services and some equity-related reporting in the general comments section above.

Response to Specific Questions – Other

This section addresses other questions or requests for comment raised within the proposed rule, excluding specific RFIs

We seek comment on whether CMS should propose to require the use of these IGs for previously finalized and proposed APIs in future rulemaking and other ways that we could support innovation and interoperability.

See our general comment above. We are favor requiring the use of specific implementation guides whenever possible. We understand that some of the guides are still changing and that backwards compatibility is not a

priority for FHIR in general and most specific IGs. That's unfortunate. We suggest CMS work with HL7 and other organizations developing IGs to help them prioritize backwards compatibility in the future. This is a standard component of nearly every other public-facing API across other industries and its lack is a significant problem for FHIR adoption moving forward. It is a fundamental requirement that client applications can continue to use older versions of APIs when the API server is updated or vice versa. New features are added separately without removing support for older, less ideal methods for doing the same or similar things should they already exist in the previous version. Until this mindset is adopted by the industry, problems around incompatibility, consistency, and adoption will abound and the types of issues you grappled with in this rule will continue unabated.

This situation is not going to change in the immediate future which leaves less than ideal options on the table – a choice between not adopting any standards or adopting less than perfect standards that will require more frequent and coordinated updates than are ideal to progress – and perhaps more frequent rulemaking than we'd prefer to accommodate that progression. We feel that the adoption of standards is the lesser of two evils in this case, particularly if accompanied by a plea to prioritize making future changes to FHIR and IGs using it in ways that are backwards compatible whenever possible.

Response to Request for Information: Accelerating the Adoption of Standards Related to Social Risk Factor Data

This section addresses specific questions asked in this RFI.

What are the challenges in representing and exchanging social risk and social needs data from different commonly used screening tools? How do these challenges vary across screening tools or social needs (for example, housing or food access)?

One major challenge we see is that different screening tools have similar but slightly different questions that can lead to very different answers from respondents – but often the responses are treated identically by those who collect, collate, exchange, and use the data.

For example, we have seen three common screening tools using versions of the following questions to screen for food insecurity:

1. Have you had trouble affording food in the last X days?
2. Have you had trouble affording nutritious food in the last X days?
3. Have you had trouble acquiring the food you need in the last X days?

Questions 1 and 2 assume that the reason for food insecurity must be financial and do not allow for respondents to indicate they are food insecure for other reasons while question 3 doesn't assume any specific reason for food insecurity.

Questions 1 and 2 also are very different despite only a single word difference in their text. Question 2 makes assumptions that the respondent is trying to seek out food that qualifies as nutritious by some unstated criteria. While in theory the goal should be the ability to acquire nutritious food, many people do not prioritize healthier eating. While that may be for financial reasons, it may also be related to cultural preferences, food availability within their preferred or available shopping outlets, or other reasons.

Someone who is food insecure because of a disability may answer no to questions 1 and 2 and yes to question 3. Someone who is not prioritizing nutrition or who isn't sure how to define it in context might answer yes to questions 1 and 3 but may not be willing to answer question 2 at all.

Despite these differences, in many cases all three questions are likely fed into the same data element in most systems, one marked food insecurity status. While some questionnaires have corresponding LOINC codes that specify the question asked, versions 1 and 2 of the question are often considered similar enough to use the

same code. Giving screening tool questions codes is only helpful if the codes are only used for exact matches – bad data is worse than no data at all, and specifying that someone answered question 1 when they actually answered question 2 is not helpful.

Another prevalent issue is an assumption of the cause of an SDOH issue, as per the assumption that food insecurity must be a financial issue when there are quite a few other reasons someone might be food insecure. Similarly, some people tend to assume transportation insecurity is predominantly a rural issue and that the main solution to transportation insecurity is providing better public transportation access, perhaps by buying tickets or passes for individuals. Anyone who has actually relied on public transportation can tell you that public transportation comes with a great deal of transportation insecurity and is not a magic solution.

We have not seen anyone prioritize collecting and sharing the cause of various SDOH issues, but without this data it is impossible to determine an effective intervention.

Finally, we also note that people tend to treat SDOH issues independently, but in reality they are often connected to each other and may have common causes or one factor will cause an issue with another. For example, someone who is disabled may be transportation insecure in a way that exacerbates food insecurity. Signing that person up for access to a food bank is likely not going to be a viable solution for them – they need a solution that revolves around mitigating the affects of their disability in ways that help them with both transportation and the subsequent acquisition of food they can use (if their disability limits the way they eat).

What are the barriers to the exchange of social risk and social needs data across healthcare providers?

In addition to collecting the data in ways that have meaning to others (as addressed above), consent and varying comfort level with different providers may be a limiting factor. We understand this data is part of USCDI v2 and already optionally allowed to be exchanged via payer APIs and supported by certified health IT, but almost every person we've discussed SDOH data with feels like it should be considered protected data on the order of behavioral health and substance abuse data and does not want it to be automatically exchanged with anyone. Doing an exchange without consent is likely to alienate the people you're attempting to help, causing loss of trust and disengagement from any SDOH-related discussions.

Another issue is that most people feel strongly that a provider or payer should not collect SDOH data if they do not have programs designed to address the issues they ask about. If you do not have transportation programs, don't ask about it. However, this assumes that the provider or payer (or community organization) collecting the data is the one who will be acting on it. That may not be the case, but patients still have the same expectation.

These are not technical barriers, but that does not make them any less real. We strongly urge CMS to consider these types of issues and concerns in any SDOH-related programs or rulemaking they pursue even though ONC standards already build in expectation of automatic exchange of some of this data.

What mechanisms (EHRs, Health Information Exchanges [HIEs], software, cloud-based data platforms, etc.) and/or standards are currently used to capture, exchange, and use social risk and social needs data? What challenges, if any, occur in translating, collecting, or transferring social risk factor data in these platforms to Z codes on claims

In general, coding systems are greatly inadequate for capturing SDOH data (see some specifics in previous comment). Among the biggest problems are a lack of identification of the underlying cause of an issue and no way to document it when one is identified. Z codes are very general, are somewhat focused on social and family-related issues, and do not adequately convey much if any of the useful information about an identified SDOH issue. For example, until 2023 they did not even support a specific transportation insecurity code and the taxonomical hierarchy of both the food insecurity and transportation insecurity codes imply that the only reason for either issue is financial. Even if a Z code exists, most of the related information is lost. This may be sufficient for claims data, but it does not represent good patient data for treatment/intervention purposes and should not be the basis of data sent by payers to others for treatment/intervention use or for interpretation in clinical or community service settings.

What privacy issues should be considered when formulating policy for collecting and exchanging social risk and social needs data? Are there certain data elements that patients may wish to exercise more control over than others?

As noted above, nearly to a person everyone we've discussed SDOH-related data with believes it should be protected at the same level as behavioral health and substance abuse data, requiring explicit patient consent to exchange. Further, there is a tendency in some quarters to collect this data for the sake of collecting it because it's a hot topic and they feel having data is better than not having it even if no interventions are supported which exacerbates desires to restrict data availability and reduces willingness of some to engage in related data collection.

Please identify opportunities and approaches that would help CMS facilitate and inform effective infrastructure investments to address gaps and challenges for advancing the interoperability of social risk factor data.

The largest gap is in exchange with community service organizations providing services in various SDOH realms. Most of these organizations know nothing about FHIR or other standard health IT mechanisms, applications, and tools. Encouraging some level of API interaction with these organizations for referrals and related supporting data is essential; FHIR is the logical mechanism for doing so if some basic level of FHIR support could be integrated into their existing computer systems.

Response to Request for Information: Electronic Exchange of Behavioral Health Information

This section addresses specific questions asked in this RFI.

Would small practices and community-based providers be able to more quickly adopt applications using API technology to exchange health information when the technology is not tied to an EHR?

There is no reason at all APIs need be tied to EHRs. In fact, this is exactly the same issues outlined above in the SDOH RFI – integration of FHIR APIs and related data into existing IT systems not currently using it. Both issues can be solved via development of lightweight applications that send/receive FHIR from the outside and convert it to/from whatever the data formats being used are. This is easier if there is standard software or formats for behavioral health (or in the case of the SDOH cases, food banks or homeless shelters or...) but could still be managed with somewhat more effort even if that's not the case.

What levers could CMS consider using to facilitate greater electronic health data exchange from and to behavioral health providers?

There are two separate considerations here: making a patient's other health information available to behavioral health providers and making behavioral health information available to other parties. For the first, a lightweight solution such as that discussed in the last comment should be sufficient. For the second, the better question might be whether this is a valid goal given restrictions on this data exchange. While exchange from behavioral health providers to others is allowed with patient consent, it does currently require patient consent so it would still need to be segregated or tagged in some way in the receiving location should permission to send it there be granted. However, the goal of electronic exchange of structured data over more manual/document-based forms of information exchange is still valid. There is nothing inherently different about such exchange other than the additional consent requirements. We suggest development of an IG that focuses on the consent considerations and some mechanism that ensures consent requirements are respected after data transport.

Are there particular considerations for electronic data exchange for behavioral health providers who practice independently, are community-based, or are non-

traditional providers?

Depending on their setting and practice type, some of these providers may not even use computers beyond managing the business elements of their practice. For example, someone who offers counseling through a church or community center may be sitting in a random room somewhere used for other purposes much of the time and prioritize eye contact or engagement with the patient over taking notes. In these cases, there may be no or extremely limited written notes which are more likely to be on paper than electronic to ensure the note taking isn't a distraction to either party. In other cases, there may be an agreement to limit the types of data included in notes to make the patient more comfortable with discussing certain topics. In this case, the behavioral health provider may have access to data from other sources but not generate much data that could be sent to others.

Response to Request for Information: Improving the Exchange of Information in Medicare Fee for Service

This section provides a general comment about this RFI

Applicability of questions to Medicare vs other payers

When reading this RFI, we were struck with a sense that all of questions being asked in the context of Medicare are not specific to Medicare in any way. It seems like a more general approach that could be used for relevant data exchange between providers, medical suppliers, and any payer would be helpful for all. Perhaps CMS could look at encouraging a related use case at one of the FHIR accelerators (perhaps DaVinci would be interested) that would include coordination between the three parties (or four as it may also be appropriate to send some data to patients for their records).

We note that many aspects of the situations outlined in the RFI also apply to any situation where there is an ordering provider and some other person or organization actually providing the service whether that's a specialty provider or radiology or laboratory services or procedures or...

Additionally, we wonder if some of the ongoing work looking at supporting communications between a convening provider and secondary providers for the No Surprises Act could be leveraged for this purpose as well.

Response to Advancing Interoperability and Improving Prior Authorization Processes for Maternal Health

This section addresses specific questions asked in this RFI.

What are key gaps in the standardization and harmonization of maternal health data? How can HHS support current efforts to address these gaps?

Our DGC participants point out that most deliveries in Massachusetts are submitted on a global bill that includes all prenatal and post-partum care. Specific dates of services are not always available and it can be difficult to calculate post-partum care from claims; at the current time EHR access is often required for payers to get this information. Among other issues this type of data flow can make it difficult to identify high risk pregnancies or provide interventions.

Adding specific requirements to exchange more specific pregnancy-related data via FHIR APIs would be extremely beneficial and allow payers to ensure they're properly providing post-partum coverage for the full allotted/supported time period as well as offering all available intervention programs for high risk pregnancies.

We believe that observations as a class should be added to USCDI, but barring that, defining specific pregnancy-related observations to include for a mandated exchange via either USCDI or USCDI+ would likely be a helpful exercise. We do not have specific insight into exactly what data would be most helpful to include

for this purpose

Response to Advancing the Trusted Exchange Framework and Common Agreement (TEFCA)

This section addresses specific questions asked in this RFI.

How could the requirements of the Common Agreement and the QTF help facilitate information exchange in accordance with the final policies in the CMS Interoperability and Patient Access final rule ([85 FR 25510](#)) around making clinical and administrative information held by health plans available to patients? How could TEFCA support proposed requirements for payers under this rule related to provider data access and prior authorization processes?

We believe that TEFCA in its current form is not particularly relevant for this rule. While TEFCA has some support for payers and for patient access, its clear primary focus is on provider=>provider exchange. Further, it is primarily a document-focused exchange using C-CDA at this time. There isn't an obvious or easy way to translate data acquired in this format into structured data that could be used within the Patient Access API, Provider Access API, or Payer=>Payer API. We understand TEFCA has a FHIR roadmap and perhaps in the future when it is further along this path it might be a reasonable avenue for FHIR exchange.

How should CMS approach incentivizing or encouraging payers to enable exchange under TEFCA? Under what conditions would it be appropriate to require this approach by payers subject to the proposed regulations in this rule and previously finalized regulations in the CMS Interoperability and Patient Access final rule ([85 FR 25510](#))?

We do not believe CMS should be encouraging TEFCA use for anything related to this rule. See the previous comment.

What concerns do commenters have about potential requirements related to enabling exchange under TEFCA? Could such an approach increase burden for some payers? Are there other financial or technical barriers to this approach? If so, what should CMS do to reduce these barriers?

We recommend CMS encourage TEFCA to prioritize FHIR support if it believes TEFCA is or could be a viable vehicle for FHIR data exchange as outlined in this rule and to consider how it could be more focused on ensuring the data required for these exchanges is supported and available via TEFCA in FHIR data formats in a consistent way. As long as C-CDA remains a primary focus of TEFCA we believe that real FHIR exchange will remain difficult at best.