Massachusetts Health Data Consortium

CMS Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard (CMS-0053-P) Comment

This document is submitted by the Massachusetts Health Data Consortium (MHDC) and its Data Governance Collaborative (DGC) in response to the CMS Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard (CMS-0053-P) posted in the Federal Register on December 22, 2022 and found here: https://www.federalregister.gov/documents/2022/12/21/2022-27437/administrative-simplification-adoption-of-standards-for-health-care-attachments-transactions-and

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

Executive Summary

The feedback provided below falls into two categories:

1. Coordination of rules: ensure this rule is in alignment with Advancing Interoperability and Improving Prior Authorization Processes proposed rule (CMS-0057-P) and other rule making
2. FHIR: support FHIR as both a data format and exchange mechanism

General Comments

Since CMS did not explicitly call for comments on particular items or in different portions of the rule, this section contains all of our comments, both on the general approach taken and on specific aspects of the 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 interoperability and prior authorization rule, Advancing Interoperability and Improving Prior Authorization Processes proposed rule (CMS-0057-P). This 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 CMS-0057-P (“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 attachment 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 (more on this below).

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.

Support for FHIR attachments

We note that the original proposal for the current recommended standards for attachments was outlined in 2016 in an NCVHS letter to the then Secretary of HHS. This letter was written nearly seven years ago and standards for data and data exchange have changed in the interim.

More and more healthcare data exchange is moving to FHIR APIs. This is happening both because of regulation and for business reasons driven by savvy organizations that understand the power of APIs. However, we acknowledge that the industry as a whole is not yet ready to use FHIR as its sole mechanism for data exchange (even if HIPAA requirements permitted it). Different organizations are further along the FHIR pathway than others, but all organizations should be on the journey soon if they have not started already. Both CMS and ONC regulation promote and/or require FHIR use as both a data format and an exchange mechanism for a variety of purposes, particularly when it comes to clinical data exchange (but also for some administrative and other data as well). Attachments are very much about the exchange of clinical data and, as such, should also be considering this industry-wide change.

Further, attachments do not currently suffer from the same drag as many other types of data – widespread existing production deployment of X12 mechanisms. We believe it would be a shame not to take advantage of this by allowing those organizations that are ready to use FHIR for attachments to do so. Requiring them to create new X12/C-CDA solutions at a time when the industry is starting to transition to FHIR makes absolutely no sense to us, especially when it would be done solely for regulatory compliance and not to meet any business need or long-term industry goal.

We understand that organizations that do not currently use FHIR and are not currently under mandate to do so in the near future may benefit from expanded use of X12 (as might some organizations with existing internal resources and expertise around X12 and other EDI mechanisms while they ramp up their FHIR support and expertise) but the goal should be transitioning organizations to FHIR if and when possible. This is not only so they can reap the benefits of FHIR, but to limit extra burdens in place around data mapping, maintaining

multiple systems, and retaining expertise and resources in both EDI and FHIR during a transition period when both technologies are in general use.

Thus, we propose the current rule support both the outlined approach of X12/C-CDA attachments and attachments using FHIR for both the data and the exchange mechanism. We also propose development of a glidepath toward transitioning fully to FHIR at some point in the future.

In addition, we respectfully request CMS clarify how the process of requesting supporting documentation for a prior authorization request should work if the PARDD APIs outlined in CMS-0057-P are adopted for electronic prior authorization processing and X12/C-CDA are adopted for attachments. The two do not seem entirely compatible on the surface as one specifies using FHIR for requesting and supplying specific documentation needed to support a prior authorization request (the DTR component of the combined PARDD APIs) and the other tells organizations that they must send the data supporting prior authorization requests in X12/C-CDA attachments.

Data Provenance

One concern we hear repeatedly from payers about 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. Further, data acquired by a payer via the attachment process likely must be included in the various mandated API calls. Thus, we propose that all attachments support the inclusion of provenance metadata. This metadata 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 gathering more information or clarification about data from its original source or the source of any modifications as well as for tracking down errors in transmission or translation from system to system if needed. We believe a standard provenance format should be defined for this purpose that can be represented within either C-CDA or FHIR.

Information Used to Make Prior Authorization Decisions

One of the requirements of the Patient Access API, Provider Access API, and Payer=>Payer API in Advancing Interoperability and Improving Prior Authorization Processes proposed rule (CMS-0057-P) is inclusion of all information used to make the prior authorization decisions. We respectfully suggest that FHIR support for attachments would be helpful here as well. We note that this rule currently requires the use of X12 275 transactions with C-CDA data for attachments and the APIs in CMS-0057-P require the same data be available for exchange via FHIR APIs using FHIR data resources. 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 reuse 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 data format requirements of the two rules as currently defined increase the burden on payers. 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.

Use of LOINC Codes to Represent the Requested Attachment Data

The proposed rule indicates that LOINC codes must be used to indicate the information being requested or transmitted via attachments as follows:

1. To identify the specific kind of information that a health plan electronically requests of a health care provider and a health care provider electronically transmits to a health plan; for example, a discharge summary or a diagnostic imaging report.
2. To specify certain optional modifier variables for attachment information, such as, for example, a time period for which the attachment information is requested.

3. For structured attachment information, to identify specific HL7 Implementation Guide: LOINC Document Ontology document templates.

We respectfully propose that purpose #1 explicitly support using DTR (or the PARDD equivalent) for requesting and gathering specific prior authorization information needed to support a PA request, that FHIR API query parameters be supported for specifying timeframes or similar constraints per purpose #2, and that purpose #3 allow the specification of a particular FHIR implementation guide to use for the data (perhaps with US Core allowed by default) instead of HL7 document templates.

At a minimum, discussion of how the process of requesting supporting documentation via the DTR functionality of the PARDD APIs fits in with the idea of using X12/C-CDA attachments is warranted. CMS is requiring FHIR use for automating electronic prior authorization requests with one hand, including requesting and supplying specific documentation needed to support a request, and telling organizations that they must send the data supporting prior authorization requests in X12/C-CDA attachments with the other hand.

Electronic Signatures

The standard FHIR exchange mechanisms include strong identity and authentication mechanisms which we believe should be sufficient for FHIR-based attachments given that they are sufficient when sending the same clinical information via FHIR generally.

However, if this is not deemed sufficient, the addition of Provenance resources with the specific clinical approver's information could be used to verify the clinician has signed off on the PA request. We believe that Provenance resources should be part of all FHIR exchange and provide a chain of custody for data that helps identify its original source, how it was obtained, the author of any changes/edits, the identity of everyone who has had custody of the data, and its validity. Using them to indicate a specific clinician who signed off on a specific activity would be in keeping with this approach.

There are also mechanisms for including digital signatures within Provenance resources if needed although this seems like overkill to us. These could be used to verify that the clinician initiated the PA and that they signed off on information shown to be included in the request in the user interface of their EHRs, SMART on FHIR apps, or other software (but the transaction itself likely would not be reviewed but rather automatically generated based on the approval via UI- this, too, would almost certainly be true for any transport mechanism).

The use of authentication and provenance (with or without digital signatures) would meet the 3 requirements for the transaction itself as follows:

1. User identity: OAuth 2.0 and other standard authentication requirements provide verification of the source of FHIR API requests.
2. Message integrity: Physician can sign off on information to send for a prior authorization or claim request and, if desired, the system can generate Provenance resources supporting this designation (with or without formal digital signatures).

   This step would be identical for the clinician regardless of the exchange and data mechanisms used and verifies the information the clinician intends to be included in their normal workflows, not their review of the actual messages to be sent. The strength of this, in all cases, is dependent on activity logging and accuracy of the EHR and other software used as the interface between the clinician and the back end message generation processes.
3. Nonrepudiation: The actions of a clinician signing off on any order, prior authorization request, service, or anything else should be logged in system of creation in a way that cannot be altered. Similar interactions should occur on the payer side when they initiate message traffic. This is independent of the data format or exchange mechanism used. This should, in theory, be a requirement before initiating any message traffic. Provenance resources attesting to this type of logging could be generated and included in the exchange.

   Again, regardless of the data format and exchange mechanism, the strength of this is dependent on the configuration, logging, and accuracy of the EHR or other software used by the clinician to

review the data and sign off on it. It is a data governance function of the organizations involved. This is true regardless of the presence of digital signatures, authentication tokens, Provenance resources, or any other mechanism used to identify and verify electronic exchange and the data therein.

We note that regardless of the transport mechanism, data fidelity moves under recipient control once it's obtained and received data could be modified entirely outside of the attachment framework. What is being verified in all cases is the integrity of the received message. Additional governance measures within payer and provider organizations may be desired to ensure message content is properly managed after receipt.

We urge careful thought in how incoming messages are logged, tracked, and transformed. For example, if incoming FHIR traffic is transformed into another format prior to storage, logging of incoming IDs and associations between the data should be encouraged (at a minimum). If being stored as new FHIR objects in the recipient system with different IDs, storing the incoming IDs under the identifier property of the new objects should be encouraged to allow reassociation with the origin system if needed. Creation of new Provenance resources containing links to a chain of the previous Provenance resources pertinent to the data should also be considered to maintain a chain of custody/full history of the source of data. These should also associate former IDs with current ones and store similar historical tracking information. We note these activities happen within the black box of the recipient of the data and are governance functions therein, not part of the exchange itself.

While we approve of extensive logging of message traffic, we also urge careful consideration of the exact content logged and how logs are stored and accessed, especially in production or cloud environments. There is some amount of increased danger around breach or misuse inherent in logging contents of messages containing PII and PHI, both in terms of increasing the number of places containing the data and because bad actors will sometimes explicitly look for such files as easier ways to acquire larger amounts of useful data. We also note that such logging may be difficult or impossible with encryption mechanisms in place.

Proposed Compliance Dates

We propose that the compliance date for this rule be aligned with the compliance date for CMS-0057-P to ensure a comprehensive prior authorization solution can be developed and implemented together rather than piecemeal and so that an entire solution be in place from the start rather than requiring modifications to the process as in place for the first rule once the second one becomes effective.