Note: All comments in Zulip and in this document are made as an individual contributor/community volunteer to advance interoperability. My goal is to share technical issues and design flaws as a gesture of goodwill toward the community.

I am requesting modifications to the CMS rules that would reimagine payer-to-payer and payer-to-provider information exchanges as a member centric exchange. Instead of member facilitated payer-to-payer and payer-to-provider exchange networks we can achieve the same effects, more efficiently, and more securely by using member centric exchanges instead. Member centric exchanges seems favorable to all parties, especially the member/patient. This proposal will simplify data exchanges drastically while delivering a superior product, but would require modifications to the following rules:

- Final: CMS Interoperability and Patient Access final rule (CMS-9115-F)
- Proposed: Reducing Provider and Patient Burden by Improving Prior Authorization Processes, and Promoting Patients' Electronic Access to Health Information CMS-9123-P

The 1/1/2022 payer-to-payer and the prior auth proposed rules cannot be implemented securely by payers until a few key pieces of infrastructure are in place. There are at least three healthcare infrastructure challenges and some procedure issues that preclude the creation of a healthcare peer-to-peer network. Currently the payer community can only securely communicate healthcare data through business-to-business connections and directly to our members/patients.

The payer implementer community does not possess a uniform understanding of the specific implementation details for payer-to-payer and payer-to-provider connections and transfer of data. Technical issues were overlooked or understated. We are rushing to implement industry wide changes with no clear benefit to our patients/members, the primary individual this rule is intended to benefit. Furthermore, I believe the community has made a mistake by removing the member/patient from the center of healthcare data transfers. The data transferred for the interoperability use cases is for the benefit of the member/patient. We are introducing unnecessary complexity, introducing security vulnerabilities, increasing implementation costs, and delivering an inferior product to our patients/members.

The technical issues are as follows:

**1.) There is a better solution**

The solutions proposed for payer-to-payer and payer-to-provider are needlessly complex. We did not seem to consider using the application development ecosystem to help solve some of the industry-wide problems impacting the member directed exchange of healthcare data between healthcare data holders. Using an application, like Apple Health or Common Health, will enable you to have access to all your healthcare information in a single location.

A patient centric approach is vastly more secure than the proposals made to facilitate payer-to-payer exchanges of data. I have not yet heard discussions about how we plan to support payer-to-provider, but I am confident it will be even more challenging than setting up a payer-to-payer, member facilitated, exchange network.

The payer-to-payer use cases for 1/1/2022 can be met with minimal effort by the application developer community and the payers and with no additional effort from the member/patient. The primary objective of the 1/1/2022 payer-to-payer use case is to allow a patient/member to have a single place to access all of their healthcare data. This use case is met by connecting an aggregator application to all data sources. Introducing payers into the mix, to aggregate payer data, does not simplify the process for patients/members.

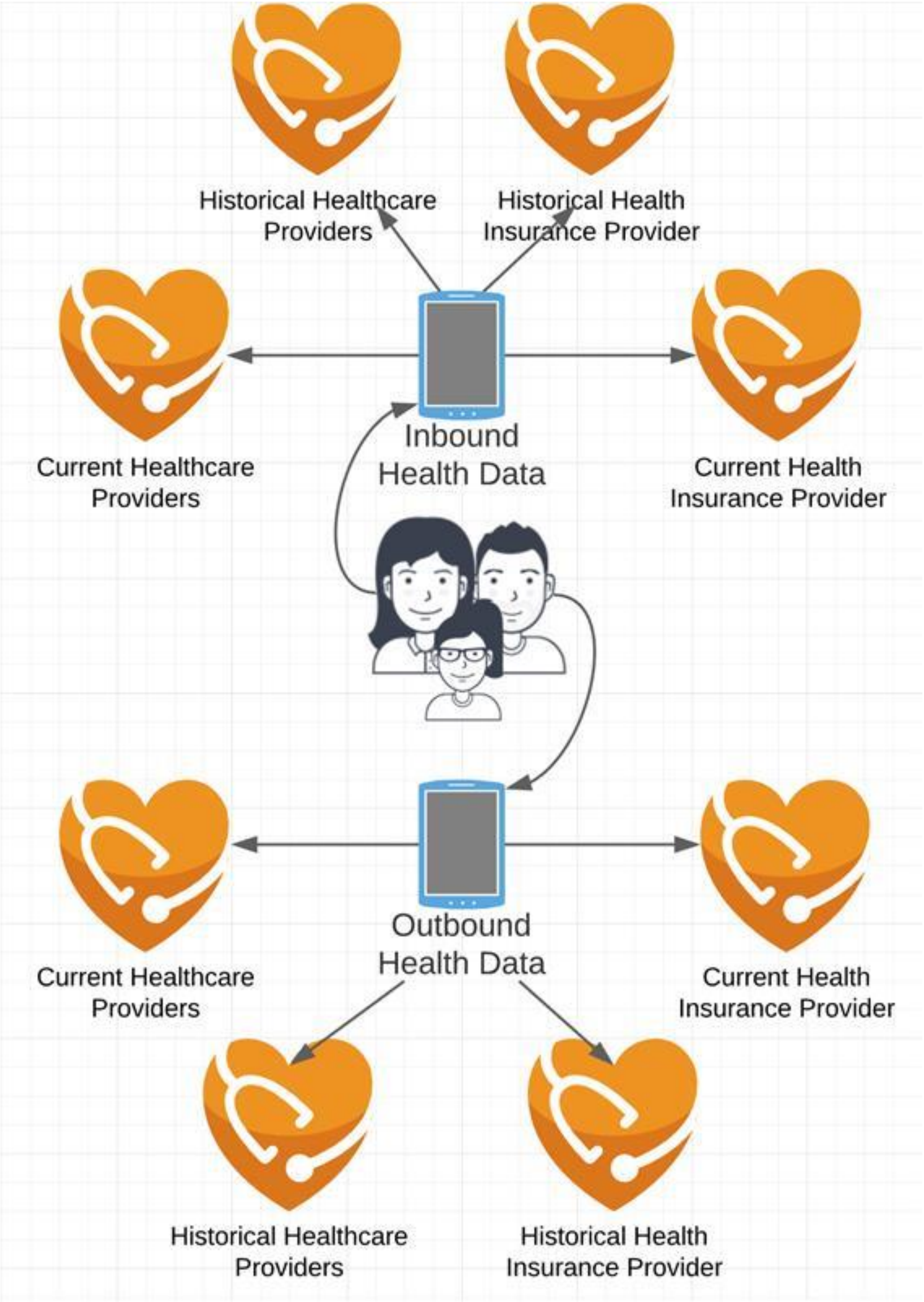
The current suggested approach, where members get their historical data via a payer-to-payer and payer-to-provider exchange network, necessitates the following:

- The creation of complex trust and endpoint discovery frameworks. Once consensuses is formed on how these will work, awareness of this process will need implemented by all data holders.
- Industry wide-consensus on how to identify and validate access to healthcare data will also be required. Efforts to achieve this have been ongoing for at least 20 years.
- Every healthcare data holder will be required to create a FHIR application. This application will register with all other data holders and it will intermediate the transfer of data from the data holder's system to external health systems. It is also important to note that an application developed on top of a single data source is of minimal use when compared to an application developed to interface with multiple data sources. A payer or provider developed application will only service the needs of a single data source. A consumer centric application will service the needs of all members/patients, allowing economy of scale.
- Limiting the patient's/member's ability to choose, at a granular level, what information to share between payers/providers
- Requires that payers receive data in non-FHIR formats from prior payers, which will prevent true interoperability
- Requires that payers and providers build out infrastructure that is only accessible through an insurance provider

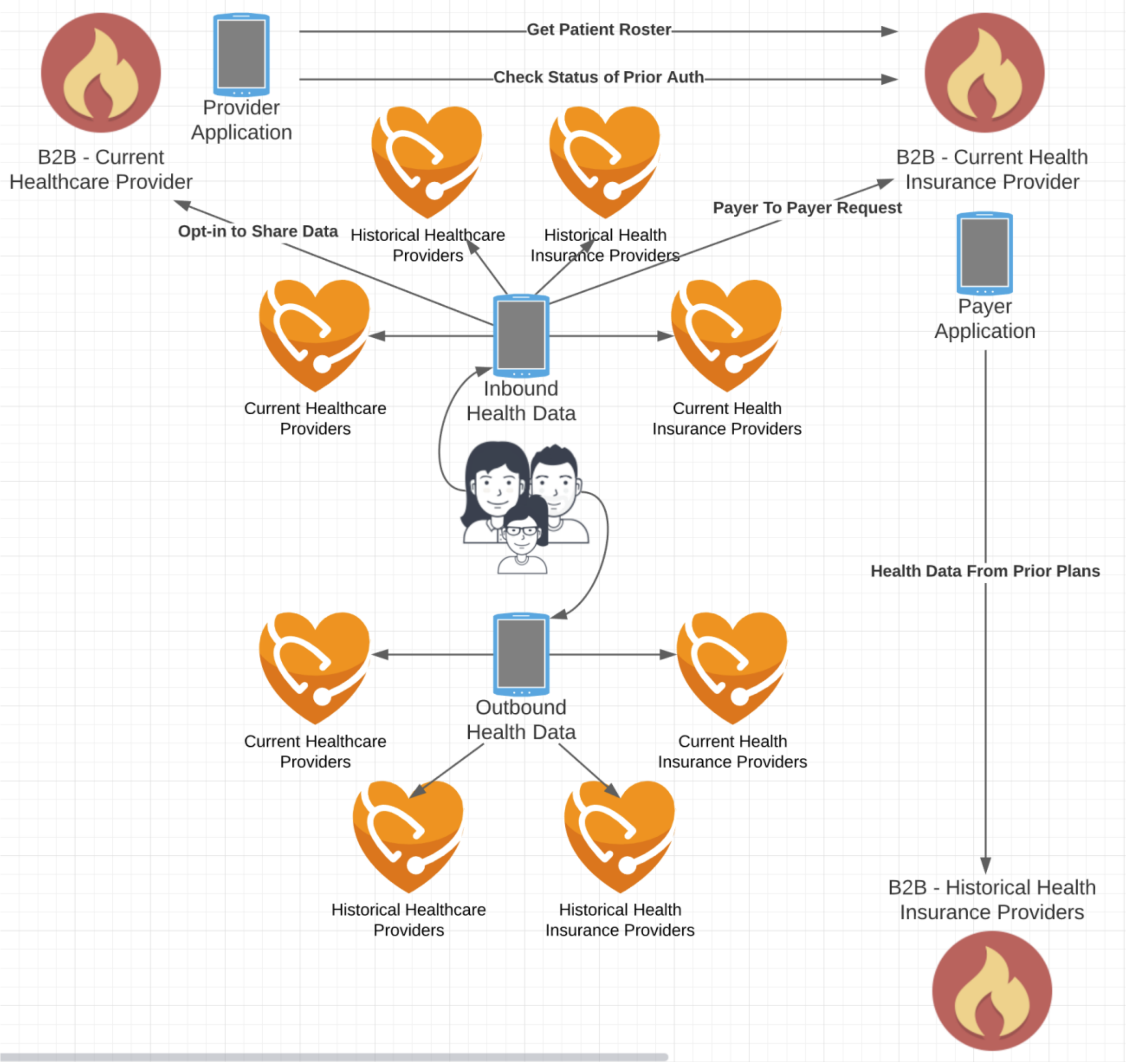
We can meet the payer-to-payer use cases without creating any new payer-to-payer or payer-to-provider connections. The advantage of this approach is that it allows all healthcare data holders to use existing connections to communicate with the only entity in healthcare that everyone has already agreed to trust, our patients/members. This approach also places the patient/member at the center of all healthcare data transactions, both in a literal and figurative sense. Additionally, this approach is widely supported by industry leaders like Apple Health and Common Health, both of which seem well situated to add support for Payer-to-Patient and Patient-to-Payer/Provider flows. This approach is also superior because it allows application developers to focus on writing code, instead of building out and maintaining thousands of connections.

In a patient centric model, all connections are established by the patient. An application will be able to utilize the connections that a patient/member has made to help mediate the transfer of data from patient-to-provider and from member-to-payer, etc. The patient's/member's authorization to release data will be implicit through the application's terms of use, and by the patient/member agreeing to share the data.

The following image depicts a patient centric flow:


Historical Healthcare Providers
Historical Health Insurance Provider
Current Healthcare Providers
Inbound Health Data
Current Health Insurance Provider
Current Healthcare Providers
Outbound Health Data
Current Health Insurance Provider
Historical Healthcare Providers
Historical Health Insurance Provider

The current proposal to address payer-to-payer and payer-to-provider data flows do not simplify things for the member/patient. The following diagram represents my best estimation of the eventual intent of payer-to-payer and payer-to-provider data exchanges:


Provider Application
Get Patient Roster
Check Status of Prior Auth
B2B - Current Healthcare Provider
B2B - Current Health Insurance Provider
Historical Healthcare Providers
Historical Health Insurance Providers
Opt-in to Share Data
Payer To Payer Request
Payer Application
Current Healthcare Providers
Inbound Health Data
Current Health Insurance Providers
Health Data From Prior Plans
Current Healthcare Providers
Outbound Health Data
Current Health Insurance Providers
Historical Healthcare Providers
Historical Health Insurance Providers
B2B - Historical Health Insurance Providers

## 2.) The patient should be the front door for healthcare data, not the payer

Clinical data that is rolled over from payer-to-payer will always be incomplete. The concept of using the health insurance provider as the front door of health care is flawed. The patient/member is the front door of healthcare data, especially in member facilitated exchanges between data holders. A payer will be unable to represent a full medical picture. Payer's will already be exposing all the clinical, claims, and formulary data they maintain through the Patient Access API. Requesting prior payer data from the current payer does not simplify the process for anyone, especially since the process must be member facilitated and they are required to provide identifying information about the prior plan. Using the same amount of effort, the patient/member should be able to provide credentials (or retrieve them) from the prior payer. If an inability to retrieve credentials for a prior plan is the issue, we can address this issue more directly than by creating a peer-to-peer healthcare exchange network.

The clinical data a payer maintains will be incomplete because payers will only consume the data they need to support business processes. This may be a small subset of the patient's clinical data. If you use a patient centric model, the patient will connect to the healthcare providers directly. This will give the patient full control over the data and provide a fuller medical picture. If there are complexities around identity management (remembering portal credentials) due to frequent plan changes, we can address this issue head on through other initiates. Removing the patient/member from transactions does not help solve the issues that are present in identity proofing / authorization in a cross-system compatible way.

Another common objection to patient-centric exchanges is that the patient/member is an unreliable actor in healthcare. I agree that whatever solutions are delivered must be easily implementable by a wide variety of patients. The technology, when fully mature, should do this heavy lifting. Interacting with your health data in a way to enable continuity of care, rather than episodic care, should not be labor intensive for the patient/member.

## 3.) Endpoint Discovery and Trusted Connections

Payer-to-payer and payer-to-provider will require peer-to-peer trusted communications. Each payer will need to be aware of all other trusted endpoint's and be able to associate a member request with one of these trusted endpoints. This obstacle is being addressed through efforts such as UDAP (Unified Data Access Profiles).

A trust framework, like UDAP, will solve the issues of endpoint discovery and trusted connections, but this approach has not been universally agreed upon in healthcare. Once consensus is formed, a considerable nationwide lift will be required to implement UDAP for all impacted healthcare data sources. Manual processes and case-by-case application vetting can be used instead of an automated process like UDAP. The number of connections and maintenance costs associated with a manual approach will be untenable however.

Peer-to-peer connections also necessitate that each payer/provider creates an application and registers that application with every other impacted healthcare data holder. The payer will also have every other data holder registering an application with the payer. This web of connections assumes a lot of trust and, if poorly implemented, seems to introduce significant security risks. These risks would be in addition to the risks outlined below.

**4.) Consistent Identifiers Across Systems**

The identifiers we use to track entities in healthcare data are not consistent across systems. For example, the patient identifier I am given at one health system will not be the same as the one I am given at another health system. This is because each system defines their own identifiers. The industry has not yet agreed upon a consistent approach. This will probably not be addressed soon. It is currently illegal to require the use of a universal patient identifier in all systems.

In payer-to-payer, the leading proposal to solve the identifier issue is to have a plan's current enrollee provide their prior plans member Id. This member Id, when combined with the member's demographic data, should enable the prior plan to locate an identifier in their system that will correspond with the person who is requesting data. This proposal may work in most cases, but it has not yet been universally agreed upon as a solution, and this solution is specific to a single use case. We would need to develop another solution to define a cross-system compatible way of identifying a healthcare provider. This will be more complex because a single provider may have multiple identities, each with different access rights.

**5.) Ability to Authorize Access**

For a system to protect sensitive data the system will need to know who is requesting the information. This will allow the system to determine if the application user making the request has access to the requested data. In system-to-system communications, like we see in payer-to-payer and payer-to-provider, all connected systems will need to know what access rights an actor in one system may have in another system. Authorization also presupposes the existence of trusted connections, endpoint awareness for all data holders and applications, and an agreed upon understanding of how to identify the requestor. I am not aware of any efforts to enable cross-system data access awareness.

The ability to authorize in a peer-to-peer system (non-member/patient centric) depends upon the following:

- Use of Trusted Connections: A trusted connection will help data holders trust that the application connecting to their system is not malicious. This implies nothing about the user of the application. If the application end user is not a patient/member, using OAuth 2.0 SMART patient scope, a trusted connection will be required. A malicious application would have too much control over sensitive information if grated business level access (ability to declare an identity). A patient/member facing application can be public, since the patient will be authorizing directly against every data holder. A business-to-business application would need to be trusted, e.g. not on an app store and not in a single page application. You would never want a business-to-business trusted application to be freely available.
- Endpoint awareness: A data holder will need to associate member / provider requests with the corresponding Business-to-business connection. The member/patient would interface with a

data holder developed application and would provide inputs to enable the data holder to locate the appropriate endpoint, e.g. They provide some identifier for the prior plan, like plan name.

- Consistent cross-system identity resolution: In order to authorize access to sensitive data the system that is providing data must be able to reliably locate an identity in their system that can be used to determine access rights.
- Cross-system role-based awareness: In a business-to-business model, the access rights of the actor/end user requesting data must be validated before releasing data. A end-user facilitated business-to-business use case creates identity challenges that are not present in in a patient/member centric model. The system providing data will not possess the identity of the requestor (in an OAuth sense) in their system. This will create a scenario where the system providing data must trust that the identity assertion of the requestor. The system providing data must also perform a demographics match, using data elements that can be easily modified: name, dob, and member Id of prior plan. This is much less secure than authorizing the member/patient/provider directly against your identity management system.

In the absence of a consistent way to validate access rights in a cross-system compatible way security vulnerabilities could be created. The burden of authorization will be placed on the payer who is providing the data. The system requesting data could fabricate identity information and effectively have access to any PHI in the sending system, if they can provide enough identity information to enable a demographics match. A malicious application user could also easily request data that they do not have access to by manipulating the request data. Given the hundreds of data sources we are adding it seems likely that at least one of the sources will introduce a vulnerability.

As stated before, business-to-business communications, in this current model, require significant trust. This is because we are creating a system where one actor can declare that they possess an identity in another system, and the other system is required to trust this assertion. A malicious application or end user could easily take advantage of this by providing identity and demographic information that will allow them access to the information they are trying to steal. Since applications can register directly with data holders and the use of a trust framework is not required, it seems that a malicious actor could create an application and manually register that application with a healthcare data holder. We are currently prohibited from blocking an application from accessing our API unless we can demonstrate a security risk to our system. This gap seems the most dangerous.

A patient centric model is more secure because the system that is providing sensitive data is also the system that is issuing the identity and validating access rights. This process will eliminate the trust issues associated with a third-party created identity. The data holder will also be able to utilize existing identity management security processes, e.g. multi-factor authentication.

### Suggestions to Meet Use Cases

A nationwide healthcare peer-to-peer network of trusted connections and actors is not required to meet the specific components of the 1/1/2022 payer-to-payer and the Prior Authorization proposed rule. We can tatisify the intentions of these rules, while delivering a better product, using member directed exchanges.

- 1/1/2022 - Payer to payer exchange of claims/clinical data: This use case can be met through the existence of aggregator applications. These applications have been building the connections that will enable a single application to connect to multiple sources. A patient/member would meet this use case by connecting the application of their choice to all historical data sources. There is no new information about a member/patient generated as a direct result of the payer-to-payer aspect of this rule so the patient would have access to all information, in one place. This approach is also superior because it will result in a more complete medical history. A member who relied on payer-to-payer data exchange to pull clinical data would only have a small fraction of the available clinical data. The data a member can access from provider sources will be more complete than the subset of clinical data that a payer may maintain for the patient/member.
- Proposed - Documentation Requirements for Prior Auths: This does not seem like it will be protected/confidential information. If so, it can be exposed through a public api, which will remove the trust and authorization issues present in current payer-to-payer designs.
- Proposed - Ability to check status of Prior Auths: A member would use an application of their choice to directly search the prior authorization status. The status could then be sent directly to the provider or communicated to the provider by the patient. This will require the creation of a new FHIR implementation guide, and this can be included as part of the patient access API.
- Proposed - Ability to communicate roster to providers: This use case could be met if all the patients relevant to the provider have connected to the provider. The provider would have a one-to-many connection relationship that is enabled by the patients that have connected with the provider. Patients that choose to connect to the provider will be able to send data to the provider, essentially building a roster that patients had to opt into (member/patient opt in)
- Seeking Comment - Ability to more easily transfer prior authorizations between payers: (Not an expert, just my hot take) Maybe we could also meet this requirement by beefing up the CARIN Blue Button Claims API to include a prior authorization indicator, e.g. a prior authorization number that is tied to a specific procedure code. It seems that this would just require industry consensus and inclusion into an implementation guide. The exchange of this data would be member facilitated, by using an application that is connected to both the old and new payer.