Part A
Beginning: Initial Payer Authorization
Ending: Member Match

Process

1- Payer A requests an access token for member match

2- Authorization Server for Payer B responds with an access token

3- Payer A calls the /Patient/$member-match endpoint

4- Payer B resource server validates the token to ensure it's valid and contains the proper scope

5- Request is forwarded to FHIR endpoint

6- Match endpoint, upon finding a match, stores record of the match internally.

7/8- Match response is sent to the client
Part B - Multi-Token Approach
Beginning: Payer-Patient Authorization
Ending: Patient Data Returned

Process

9- Payer A requests an additional access token, scoped to a patient. A member match ID is provided to assert match/consent has been performed.

10- Payer B authorization server looks up the match/consent record internally, and validates it.

11- An access token is minted to Payer A.

12- Payer A invokes the patient/$everything-pdex endpoint

13- Payer B resource server validates the token to ensure it's valid and contains the proper scope

14- Payer B authorization server looks up the match/consent record internally. Checks are performed to ensure the consent is still valid, and determines if any filters are necessary on the data returned.

15- Request is forwarded to FHIR endpoint

16/17- Patient data is returned to Payer A
Part B - Multi-Token Approach
Beginning: Payer-Patient Authorization
Ending: Patient Data Returned

Process

9- Payer A requests an additional access token, scoped to a patient. A member match ID is provided to assert match/consent has been performed.

10- Payer B authorization server looks up the match/consent record internally, and validates it.

11- An access token is minted to Payer A.

12- Payer A invokes the patient/$everything-pdex endpoint

13- Payer B resource server validates the token to ensure it's valid and contains the proper scope

14- Payer B authorization server looks up the match/consent record internally. Checks are performed to ensure the consent is still valid, and determines if any filters are necessary on the data returned.

15- Request is forwarded to FHIR endpoint

16/17- Patient data is returned to Payer A
Part B - Single-Token Approach
Beginning: Patient/$everything Invoked
Ending: Patient Data Returned

Process

9- Payer A invokes the patient/$everything-pdex endpoint using the same token as used for member match

10- Payer B resource server validates the token to ensure it's valid and contains the proper scope

11- Payer B authorization server looks up the match/consent record internally. Checks are performed to ensure the consent is still valid, and determines if any filters are necessary on the data returned.

12- Valid requests are forwarded to FHIR endpoint

13/14- Patient data is returned to Payer A