

https://rce.sequoiaproject.org/wp-content/uploads/2021/07/QTf-V1-Draft.pdf	question / page	comment by John Moehrke
	<p>Should the QTF include QHIN Message Delivery? If you believe QHIN Message Delivery should be included, how should it be technically specified? See detailed note below.</p>	<p>Today there are two viable solutions that are both not optimal. The Direct-Project, and IHE-XDR. Both of these should be encouraged within the communities and use-cases for which they are used. New use-cases can choose which of these best fits their need, likely based on their existing infrastructure. Those that already support Direct-Project will likely choose to expand use of Direct-Project. Those that have XCA/XDR capability will likely choose to expand use of XDR. The only conflict is the recipients of these messages will need to either guide THEIR community on the solution to use, or support both.</p> <p>Given that both of these are not optimal; the move to use FHIR RESTful push seems like a good place to focus first on the use of FHIR REST. There are solutions for FHIR RESTful push defined in the IHE-MHD implementation guide, and the model there is aligned with the XDS/XCA/XDR/XDM model. Use of this in a Point-to-Point push should be seen as a simple alternative over the two alternatives currently available.</p> <p>Given the QTF identified directory to enable endpoint discovery, and the more simple model provided by IHE-MHD push (using FHIR), there should be no need for Intermediaries. Where there is consideration of intermediaries, one needs to question the value being provided by the intermediary vs the complexity in routing, security, authenticity, provenance, integrity, and availability they bring forward. The fundamentals of http REST are built upon the Internet and http protocols that are world-wide, and the security of TLS that is proven.</p>

	<p>What elements should be included in a TEFCAs FHIR Roadmap to provide predictability and a clear direction for QHIN-to-QHIN exchange regarding the implementation of FHIR for QHIN Query, QHIN Message Delivery, and for enabling FHIR data to be used by Health IT systems?</p>	<p>Three distinct points on this question</p> <ol style="list-style-type: none"> 1. The current TEFCAs solution can carry FHIR-Documents with zero modification of the existing infrastructure. Not just FHIR-Documents, but any kind of content. The metadata model defined in IHE is content agnostic, focusing on use of mime-type, format-code, and fundamentals of byte-stream. The metadata focuses on enabling Privacy, Discoverability, Integrity, Provenance, and Identity. The metadata model envisioned many kinds of documents, and this is why FHIR-Documents are supported by the foundation. Further the metadata model enables relationships between different encodings of the same content so that a Query Initiator can determine that multiple entries are covering the same content with different formats. In this way a Medical Summary could be published in both C-CDA and FHIR-Document; giving the document consuming system the flexibility to choose their preferred format. -- https://healthcaresecrecy.blogspot.com/2021/08/fhir-data-in-existing-nationwide-health.html 2. The IHE-MHD implementation guide provides for a FHIR based API to the technology foundation used in TEFCAs. The use of the IHE-MHD implementation guide would enable new participants to join the nationwide network fully while they use the more modern FHIR technology stack for discovery, query, and retrieve. This solution does not affect the privacy, authentication, provenance, integrity, or availability of the content; as the solutions are all focused on making patient and metadata accessible, while preserving and being agnostic to the document content. <p>Combined use of 1 and 2 would enable the document consumer actor to not only use FHIR as the API, but also retrieve FHIR as the document content.</p> <ol style="list-style-type: none"> 3. The IHE has also defined an access methodology that breaks down the documents into FHIR Resource level entities. The IHE mXDE and QEDm offer this solution to make the document consumer even more easy. The solution makes sure to give provenance recognition to any documents that were used as source for the FHIR Resource level entities. Where multiple documents contained the entity, multiple Provenance records would exist pointing at the document. The Provenance can be used to retrieve the original document so that the context of the entity information can be understood within the document published. <p>For further details on ALL of these points, see the IHE whitepaper https://profiles.ihe.net/ITI/HIE-Whitepaper/index.html</p>
	<p>Mutual Server Authentication</p>	<p>I believe this should be "Mutual-Authentication". The addition of the word "Server" is nonsensical as only one side of the communication is a server, the other side would be the client. The word "mutual" already encompasses this concept.</p>
	<p>p.9 (and other) - Secure Channel</p>	<p>Please reference IHE-ATNA rather than TLS. If you feel the need to pick TLS, then there are named options within IHE-ATNA for the specifics of TLS 1.2, 1.3 and BCP195. The specifics of TLS are not sufficient to convey the requirements for secure channel found in IHE-ATNA.</p>
	<p>references to IHE IT-Infrastructure publications on www.ihe.net</p>	<p>Please change all links to the IHE IT-Infrastructure publications to those published on https://profiles.ihe.net</p> <p>It is good to see many of these, but there are many others that are not updated. Most distressing are links to old publications that have been moved to Final Text. i.e. footnote 8, 9, 12, 13, 17, 18, 20, 23, 30</p>

	<p>P 5 - Paragraph 4 - For within-QTF exchange, the QTF also describes high-level functional requirements QHINs must support within their health information networks. As long as QHINs are able to achieve the required functional outcomes within their networks, they generally have the operational flexibility to select appropriate standards and approaches consistent with the needs of their business environments. In limited instances, the QTF may specify a particular element of Participant or Subparticipant behavior in order to ensure consistency in QHIN-to-QHIN behavior.</p>	<p>I learn that the QTF was intended to express how depth of QHINs greater than 1 were to be handled. Yet this paragraph clearly states that this document addresses explicitly only depth of 1. Leaving out of scope what happens in either of the QHINs on either side. I learned at comment submission deadline that the QTF was intended to cover 2+ depth.</p> <p>My comments here are against what the text says, depth of 1. not against an unstated goal of depth of 2+.</p> <p>Note that IHE chose not to address depth due to the need to address simple federation first. The depth issue was a known gap, with expectation that when someone needed the depth issue resolved a new-work-item would be brought to IHE to address it. This has not yet happened. So the absence of specification is not a failure to have been specified, it is a failure to have asked for a solution that was explicitly delayed to enable experimentation.</p>
	<p>p. 6 - Instance Access Consent Policy (IACP): Policy instances (e.g., patient authorization forms) which may influence access control decisions and which can be referenced by queries.</p>	<p>Edit-- Instance Access Consent Policy (IACP): Patient specific Policy instances (e.g., evidence of the consent / authorization ceremony to a specific policypatient-authorization forms) which may influence access control decisions and which can be referenced by queries.</p> <p>Note that IHE-BPPC explains these things, using different but more specific terms. -- https://profiles.ihe.net/ITI/TF/Volume1/ch-19.html#19.2.1 The "acp" and "iacp" were vocabulary terms coined prior to specification normative publication- see XUA https://profiles.ihe.net/ITI/TF/Volume2/ITI-40.html#3.40.4.1.2.2</p> <p>CareQuality expresses the mapping of these terms as such - Access Consent Policy – is referred to in IHE XUA as the “Patient Privacy Policy Identifier” - Instance Access Consent Policy – is referred to in IHE XUA as the “Patient Privacy Policy Acknowledgement Document”</p>
	<p>p. 7 - The following actor names are specific to IHE profiles and used within the QTF with the following definitions, for full definitions please see IHE Technical Frameworks General Introduction, Appendix A: IHE Actor Definitions. 4 • Initiating Gateway: A transaction gateway that supports outgoing requests and responses for QHIN Query and QHIN Message Delivery. • Responding Gateway: A transaction gateway that supports incoming requests and responses for QHIN Query and QHIN Message Delivery</p>	<p>add to the definitions that they not just support Query and Delivery, but also Retrieve and Patient discovery.</p>
	<p>P.7 - The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119. 5</p>	<p>should consider the normative words defined in IETF RFC 6919</p>

	P. 8 - second paragraph of Document Query Scenario --- The Query Solicitation may include patient demographic information for patient identity resolution, query parameters indicating which information the provider is looking for, and/or a list of entities to query.	This asserts a use-case that combines query for documents using only patient demographics. This is not what is actually done due to the need to confirm the proper patient is identified before moving on to document metadata before moving on to retrieving the document. To skip these intermediate steps is to introduce failure modes. The text given may be considered an abstract concept, but then should be tagged as explicitly abstract or informative.
	P. 8 - mentions of TLS	should rather use ATNA, but if needing to say TLS, then please augment with ATNA. ATNA is where the TLS requirements are more fully expressed in transaction protecting form.
	P.8 - mention of TLS	should there be a mention here about certificate management
	P. 9 - standards table	Should also mention Consistent Time (IHE-CT profile https://profiles.ihe.net/ITI/TF/Volume1/ch-7.html) . Having audit logs that are not comparable is problematic. Consistent time is also critical to medical records. The requirement is likely already being adhered to, as the solution is baked into all operating systems and most have it enabled. However because of the relationship to business needs and security needs it is worth saying. -- further saying it, does then mean that there needs to be a policy on what are appropriate time sources, and what is the allowed drift.
	P.9 - standards table	There should be mention here about IHE-mCSD as the profile providing the foundation for the QHIN Directory. https://profiles.ihe.net/ITI/TF/Volume1/ch-46.html
	P. 10 - table	There is no introduction to this table or how to read it. I eventually understood that the second column is identifying how many of these actors (rows) would exist in any one QHIN interaction.
	P. 10 - table	unclear the QHIN Directory two rows. also, unclear the relationship to the RCE Directory
	P. 10 - patient demographics	Please elaborate on what is meant by "patient demographics". This term is not well understood, and some have the impression that it is nothing other than name and postal address. I believe that it is more than that in the eyes of the QTF. Specifically including gender, and other identifiers. Might want to use the definition IHE has adopted in the PMIR profile for "Patient Identity" -- All information used for identifying the patient, such as identifier, name, phone, gender, birth date, address, marital status, photo, others to contact, preference for language, general practitioner, and links to other patient identities.
	P. 10 - assumptions	Query metadata vocabulary? -- metadata handbook -- https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_Metadata.pdf
	P. 10 - assumptions	Trust fabric? Aka certificate management
	P. 10 assumptions - 2) The Query Source does not know both the patient identifier(s) and Responding QHIN(s) for a query. a) If the Patient Identifier(s) and Responding QHIN(s) are known, the patient discovery phase of the query workflow may be omitted.	this is unclear text. I think the point is that if X is known then X-Discovery is not needed.
	P. 10 - • Each Actor has the appropriate service endpoint(s) and other connectivity information for any other Actors above or below it in the hierarchy with which it connects directly. • The RCE Directory includes the organization name(s), and HomeCommunityID(s) for all current Participants and Subparticipants. Each Participant and Subparticipant is matched to the appropriate QHIN.	I find these two bullets are in conflict. If the first bullet is true, then the second bullet is unnecessary. However I think what is actually true is that the RCE is used to find the technical details

	P. 10 - unclear the distinction being made between a pre-condition and an assumption	these seem to be being used as the same concept, yet are distinct on the page.
	P. 10 - Responding QHINs know the current HomeCommunityIDs for any Responding Sources.	would the RCE Directory also be a potential way to discover the HCID?
	P. 11 - diagram	the details of this diagram seem excessive, including internal systems design. Further this diagram does not seem aligned with the numbered steps below. Align, and leverage the numbers to draw understanding. as noted at the top of the page, an eMPI is allowed, and thus the eMPI does not need to do responding discovery steps.
	P. 11 1) The Query Source sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to discover patient matches by demographics.	do you really intend to express that a Query Source can use "any" intermediary Subparticipant or Participant? I would expect that there would need to be a trust relationship here. that the Initiating QHIN would only carry out requests that were authorized.
	P. 11 (and other) - See IHE ITI TF-2b: 3.55.	references like this should not be using the "b" in "ITI TF-2(b)" anymore. The html publication mechanism that IHE ITI is currently using no longer requires us to sub divide the volumes into a vs b. These references can also be deep links into the specification including the sub-header level by number. See this example to ITI TF-2: 3.55.4 https://profiles.ihe.net/ITI/TF/Volume2/ITI-55.html#3.55.4
	P. 11 2)	should be noted that this request include security / privacy context as described in ATNA/XUA/BPPC discussion above. Including mutually-authenticated communication (ATNA), assertion (XUA) of original organization, triggering agent, purpose of use(s), and (BPPC) consent when appropriate.
	P. 11 (and other) - 2.a) The Initiating QHIN creates an audit log entry including the HCID of the Query Source and Responding QHIN(s).	These audit log messages are fully specified in the IHE specification with details well beyond the narrative here. The narrative here is okay, but a link to the specification would help your reader understand the details that should be logged. see ITI TF-2: 3.55.5 https://profiles.ihe.net/ITI/TF/Volume2/ITI-55.html#3.55.5
	P. 11 3.a) "The IHE Cross Gateway Patient Discovery [ITI-55] response contains one or more patient matches from all potential Responding Sources, including demographics and patient ID as known by the Responding Source. The response may contain multiple entries where each entry reflects a different source of information but will include only one identifier per patient per Responding Source"	P. 11 3.a) "The IHE Cross Gateway Patient Discovery [ITI-55] response contains one or more patient matches from all potential Responding Sources, including demographics and patient ID as known by the Responding Source. The response may contain multiple entries where each entry reflects a different source of information community (HCID) but will include only one identifier per patient per Responding Source community (HCID) " note that in IHE the term community is used to explain any kind of community, even communities of communities. The most basic of community is an XDS Affinity Domain, or a single organization EHR.
	P. 11 3.a) "The IHE Cross Gateway Patient Discovery [ITI-55] response contains one or more patient matches from all potential Responding Sources, including demographics and patient ID as known by the Responding Source. The response may contain multiple entries where each entry reflects a different source of information but will include only one identifier per patient per Responding Source"	The XCPD response will contain potentially multiple entries, but any assigning authority thinks that all these entries are the same human (this is the best Bob I found given the parameters you gave me). Meaning that the response can't contain alternative humans at a given assigning authority. But there is no guarantee that identity at different assigning authorities are the same human. Thus where there are identities at different assigning authorities the demographics included in the response should be compared further for match appropriateness at the initiating actor.
	P. 11 - footnote 11	url is not valid, clearly including "TBD"
	P.12 - 4.a	note an error should also be logged if errors happen. and the success audit log should not include the results returned, but should include the xcpd query requested. see ITI TF-2: 3.55.5 https://profiles.ihe.net/ITI/TF/Volume2/ITI-55.html#3.55.5

	P.12 - 4)	<p>Worthy to note that this resulting set is all the "Locations" where "Records" exist - hence the results of a Record Location system (vs service). A Federated "system" for locating Records.</p> <p>Which those places that use a universal patient identifier don't get.. but the USA does because we don't have such a thing and thus every assigning authority is effectively a "location" where data are known to exist for that patient. aka... making lemonade out of the lemons the USA has given us.</p>
	P. 12 - alternate Flow 2: step 2 -- the responding source obtains the (I) ACP..	<p>If the IACP is retrieved or not is a policy decision. There is nothing to retrieve when an ACP is provided, as this is essentially just a code for a shared Policy. Thus when ACP is all that is in the request, this is essentially the originating organization indicating that they have an instance on file, but they don't have an electronically accessible instance.</p>
	P. 11-12 -- patient matching	<p>should it be noted that all patient matching is done to the best-effort at each assigning authority. That best-effort is based on the demographics provided, and the demographics known at an assigning authority. The best-effort to match will thus have some risk of not identifying the correct human. This may result in a false-positive (a result is returned that is not the human that was intended, but was picked as the best match at that assigning authority) (note the right human may have been overlooked, or not exist at that assigning authority), or a false-negative (no result was returned when there actually was a proper match available). The risk of failure is multiplied for every opportunity to make a match. False-positives multiply for each match returned across the whole of the network. False-negatives multiply for each failure to match across the whole of the network.</p>
	P. 13 - diagram - Document Query	<p>same comments regarding the diagram being not introduced, and lacking numbered interactions so as to be referred to in description below. Also including detail not necessary to explain the QTF relevant details. Might the QTF relevant section in the middle be highlighted so as to set it off from the left and right that are not relevant (and are the imagining of the author)</p>
	P. 13 - 1)	<p>I don't think the left hand side should be described as it is outside QTF.. but if it is, then I think it is proper to include as one alternative for how this left hand side works is thru the XCA - Initiating Gateway - XDS Affinity Domain option. https://profiles.ihe.net/ITI/TF/Volume1/ch-18.html#18.2</p>
	P. 13 1) The Query Source sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to query for document metadata.	<p>do you really intend to express that a Query Source can use "any" intermediary Subparticipant or Participant? I would expect that there would need to be a trust relationship here. that the Initiating QHIN would only carry out requests that were authorized.</p>
	P. 13 - 2) The Initiating QHIN creates an IHE Cross Gateway Query [ITI-38] FindDocuments request based on the Query Solicitation and sends it via the Initiating Gateway to each Responding QHIN's Responding Gateway.	<p>the Initiating Gateway must process each unique combination of HCID and Assigning Authority independently. For each unique HCID and Assigning Authority a single XCA query is sent, and results will be returned.</p> <p>Critical fact is that XCA must query one and only one patient, which is a patient identity at an assigning authority. And that XCA has no way in the XCA query attributes to target an HCID, other than by the technical connection endpoint that is known (Directory) to respond on behalf of that HCID.</p> <p>The exception to this is that when the patient id and Assigning Authority are unique (e.g. a national patient identifier), and there are known data at multiple HCID, and there is Directory driven knowledge that those multiple HCID can be reached by using one Intermediary Responding Gateway... then one XCA must be sent to that Intermediary on behalf of that single Patient ID at that single Assigning Authority, as the XCA query can't indicate the distinction of the HCID(s). To send two XCA queries would result in duplicate results.</p>

P. 13 - 2)	should be noted that this request include security / privacy context as described in ATNA/XUA/BPPC discussion above. Including mutually-authenticated communication (ATNA), assertion (XUA) of original organization, triggering agent, purpose of use(s), and (BPPC) consent when appropriate.
P. 13 - 2a)	as stated before... query parameters are recorded, as is success / failure -- and audit message details are specified -- https://profiles.ihe.net/ITI/TF/Volume2/ITI-38.html#3.38.4.1.4
P. 13 - 3	This detail is beyond QTF. It is a reasonable design when that QHIN is an intermediary for a set of sub-QHIN; but that is a design choice. If this was cast as a intermediary QHIN, then this logic would be reasonable (much like XCPD alternative flow 3)
P. 13 - 3.a) The Responding QHIN's request includes the patient identifier as known by the Responding Source, and may include some number of query parameters.	P. 13 - 3.1) The Responding QHIN's request to the Responding Source includes the patient identifier as known by the that Responding Source, and may include some number of the query parameters.
P. 13 3.b)	same audit comments as above
P. 14 4)	good statement about policies... is this a good opportunity to express that these access policies must not conflict with the anti-blocking ? Likely should have statement that these access policies do include explicit Patient Consent (not implicit, which leads to anti-blocking)
P. 14 5.b)	same audit comments as above
P. 14 6)	Should it be noted that the initiating QHIN need only combine results when it has sent the request to multiple responding QHIN? it is this, sending to multiple, that causes the need to wait for multiple and combine the results of the multiple.
P. 14 Nominal Flow step 6)	Note that there has been some discussion of issues of multiple pathways to the exact same data. This can be detected at this point because of the fact that documents have globally unique identifiers. see https://healthcaresecprivacy.blogspot.com/2018/04/de-duplicating-received-duplicate-data.html I would however not recommend automatic de-duplication of documents using document id alone, as that might eliminate documents that are actually different but for which proper document id management had not been utilized. Note that use of the document sharing metadata elements of size/hash could detect actual identical documents.
P. 14 6)	This seems to be out of scope of QTF, but is certainly one alternative for how this left hand side works thru the XCA - Initiating Gateway - XDS Affinity Domain option. https://profiles.ihe.net/ITI/TF/Volume1/ch-18.html#18.2
P. 14 6.a)	same audit comments as above
P. 14 alternate flow 1 2) A Responding Source returns an error message (e. g., no document is found, etc.).	note that no documents found is not an error, that is a success with zero results. An error might be XDSRegistryOutOfResources. should be noted that this case is that some results are available, but some sources had errors. The given text does not make that clear. "Some results area availbe, but at least one Responding Source..." actually seems like step 2 here is really just a pre-condition for Alternative flow 1, and not really a step.
P. 14 alternative flow 1 4)	This systems design logic seems is unnecessary for QTF to indicate. Especially since the two alternatives are not given any guidance but simply stating two subflow alternatives.
P. 14 alternative flow 1 4.a)	There should be no allowance for a source that can't handle a partial success code

	P. 14 alternative flow 2 2)	as stated above, the processing by the custodian relative to the ACP or IACP is policy, and should not have mandated processing. Not harmful to express the policy driven choice to retrieve or not; but one model should not be mandated.
	General restatement of lack of step identifiers on the diagram	Given that the diagrams do not have numbers on them, it is really difficult to understand text that refers to starting or resuming at "step n".
	P. 15 - diagram	Need numbered steps. Need introduction text for the diagram.
	P. 15 - diagram	Need better diagraming methodology to isolate the QTF scope (middle transaction) from the systems design alternatives on the left and on the right. It needs to be very clear that these are system design alternatives. These alternatives may need to be diagramed so as to support narrative below, but they are not part of the central transaction.
	P. 15 1) The Query Source sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to retrieve documents.	edit - The Query Source sends a Query Retrieve Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to retrieve documents.
	P. 15 1) The Query Source sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to retrieve documents.	do you really intend to express that a Query Source can use "any" intermediary Subparticipant or Participant? I would expect that there would need to be a trust relationship here. that the Initiating QHIN would only carry out requests that were authorized.
	P. 15 1.a)) The Query Solicitation includes the HomeCommunityID(s), Repository ID(s) if known, and Document IDs at the Responding Source(s).	There is no provision for a retrieve that does not know the full triplet of HCID, Repository ID and Document ID. edit:) The Query Solicitation includes the HomeCommunityID(s), Repository ID(s) if known , and Document IDs at the Responding Source(s).
	P. 15 - 2)	should be noted that this request include security / privacy context as described in ATNA/XUA/BPPC discussion above. Including mutually-authenticated communication (ATNA), assertion (XUA) of original organization, triggering agent, purpose of use(s), and (BPPC) consent when appropriate.
	P. 15 2) The Initiating QHIN creates an IHE Cross Gateway Retrieve [ITI-39] request based on the Query Solicitation and sends it via the Initiating Gateway to each Responding QHIN's Responding Gateway.	This seems to imply that the Query Source in step 1 has requested multiple documents from one HCID. This may be a potential systems-design, but is unnecessary complexity for the QTF. The concept of requesting one document is sufficient to explain the QTF relevant transaction. systems design can take that concept and add functionality to support multiple documents and/or multiple HCID. Ultimately a ITI-39 may ask for multiple documents, but they must be from one HCID. They should be about only one patient as well.
	P. 15 2.a)	same audit comments as above
	P. 15 3) Each Responding QHIN queries its QHIN Directory to identify the appropriate Responding Source(s) and sends a request to retrieve documents, through any intermediary Participant or Subparticipants as applicable, to each Responding Source.	A Responding QHIN might be the custodian, and thus there is no need to check with a directory. Where the Responding QHIN has another QHIN behind it, it could use that QHIN Directory to discover the endpoint for the HCID. However this detail was not expressed in the previous two (patient discovery, and query for documents). So it is strange for this level of detail to only first show up on Retrieve Document. So either include this level of detail everywhere, or no where. If the logic is expressing a Responding QHIN for many HCID that are not using QHIN logic.. then this is a proprietary architecture.. something also not mentioned above.... So, this seems to be expressing right side systems design logic that is outside of scope of the QTF.

	P. 15 3.a)) The Responding QHIN's request includes the repository ID, document ID, and/or any other document metadata as known by the Responding Source	<p>If this is describe a Responding QHIN that is using the ITI-39 transaction to communicate with the Responding Participant... Then this text is wrong, as the ITI-39 transaction is the same as is found in step 2.</p> <p>If this is describing a Repository QHIN that is retrieving the document from XDS community. Then this is described in XCA 18.2.3.2 -- https://profiles.ihe.net/ITI/TF/Volume1/ch-18.html#18.2.3.2</p> <p>If however this is describing a systems design where the Responding QHIN is using pripritary means to get the docuemnt... then this is out of scope of the QTF. Possible solutions are non-standard and could be by any means.</p>
	P. 15 3.a)) The Responding QHIN's request includes the repository ID, document ID, and/or any other document metadata as known by the Responding Source	<p>document metadata is not returned</p> <p>edit: The Responding QHIN's request includes the repository ID, document ID, and/or any other document metadata as known by the Responding Source</p>
	P. 15 4) Each Responding Source returns a response with the appropriate document(s) and associated document ID(s) to the Responding QHIN, through any intermediary subparticipants or Participant as applicable	P. 15 4) Each Responding Source returns a response with the appropriate document(s) and associated document ID(s) to the Responding QHIN, through any intermediary subparticipants or Participant as applicable
	P. 15.3.b	same audit comments as above
	P. 15.5.b	same audit comments as above
	P. 16 6) The Initiating QHIN combines all IHE Cross Gateway Retrieve [ITI-39] responses into a single response and returns the response to the Query Source, through any intermediary Participant or Subparticipants as applicable.	<p>This may be a systems-design choice, but is not the only systems design choice. This is out of scope of QTF and should be removed.</p> <p>some form of processing may be done, but what kind of processing is up to the requesting actor.</p>
	P. 16 6.a)	same audit comments as above
	P. 16 alternate flow 1 2) A Responding Source returns an error message (e.g., query cannot be delivered).	This is a Retrieve, not a Query; so the example is nonsensical. see the reasonable errors in the IHE specification https://profiles.ihe.net/ITI/TF/Volume3/ch-4.2.html#4.2.4.1
	P. 16 alternate flow 1 5) an error must be recorded at both responding and initiating	no mention of audit that is necessary
	P. 16 alternate flow 2 5) an error must be recorded at both responding and initiating	no mention of audit that is necessary. Specifically the failed retrieve will have an error message recorded, the successful will have a success recorded.
	P. 16 alternate flow 3	<p>Note that even nominal flow requires security at the TLS and SAML levels. Thus the addition of a consent policy is just an attribute within the SAML.</p> <p>also as noted above, it is policy that must determine if the policy must be retrieved.</p>
	P. 16 post-conditions	<p>unclear what this is a post-condition for. It seems like it is assuming that PD, QD, and RD were executed and succeeded nominally. But these are not always going to be executed like this, and clearly are sometimes errors.</p> <p>Sometimes a process may just want to get PD and QD accomplished, where later in the day RD will happen based on human choice. And success might be that there is nothing new to Retrieve.</p> <p>It is even possible that a PD that does not find a patient is successful for what was expected, that this patient has not been seen elsewhere than their home clinic/hospital.</p> <p>This Post-condition is too specific to a specific sequence.</p> <p>It might be okay to keep this, but would need to be explained what this is a post-condition for, and why it only covers this specific sequence and this specific success.</p>
	P. 17	Should be introduced as one of many use-cases supported by the push model. It is an unusual one to be representing the interaction, where reporting to public health seems to be the more dominant one, and one that has special handling of the situation in that there are not patient.

P. 18 Table 2 Secure Channel	Should reference ATNA as that includes useful profiling of TLS and has BCP-195 named option
P. 18 Table 2 Mutual Server Authentication	Should reference ATNA as that includes useful profiling of TLS and has BCP-195 named option
P. 18 Table 2 Mutual Server Authentication	Mutual Authentication -- one is a Client the other is a Server, so no such thing as mutual server authentication.
P. 18 Table 2	Not clear that XCDR is necessary as XDR can work using Intended Recipient.
P. 18 Table 2	Note that patient identity lookup should be considered an option as it would enable better communication Note that BPPC may still be useful if the recipient needs to know the authority the initiating actor has to push the content (not as likely) These might be useful to just explain informatively
P. 18 Actors	Would really benefit from a diagram to explain this table, and the configuration being discussed.
P. 18 Assumptions 1.a)	Is this referring to a shared PKI?
P. 18 Assumptions 1.b)	How is this different than the required ATNA + XUA you have already stated?
P. 18 Assumptions 1.c)	Is this just referring to "policies exist"? It is not clear what the technical or key requirement is here.
P. 19 Diagram	This diagram is showing interactions on the left and right that are outside of the scope of the QTF. The QTF lead page made it clear it is covering only the central transactions between the two QHIN.
P. 20 2.a)	same audit comments as above
P. 20 3)	This presumes some specific of the initiating community that are outside the scope of QTF
P. 20 3.a)	same audit comments as above
P. 20 5.a)	same audit comments as above
P. 20 6.a)	same audit comments as above
P. 21) QHINs are exchange hubs	The use of the word hub is not appropriate. One architecture does use a hub network style, but a more privacy and security architecture is one that has only a central PKI and uses Mesh Network so as to prevent inappropriate exposure to PHI. The IHE profiles work best with Mesh networks, where a Hub requires adding another connection with another set of failure-modes and privacy exposure.
P. 21) "TI"	What is "TI"? This abbreviation has not been defined or introduced before page 21.
P. 21) QTF-001 All requirements pertaining to the IHE ITI Technical Framework profiles, unless otherwise specified, refer to IHE IT Infrastructure Technical Framework Revision 17.0 – Final Text, published July 20, 2020. 13	Version 18 is now available and is fully supported as normative in html publication at https://profiles.ihe.net Very few changes happened, but the new html publication is much more user friendly, and hyperlink friendly and hyperlink using. Release tracking can be reviewed using GitHub https://github.com/IHE/publications/releases
P. 21) QTF-002	Is this requirement requiring redundant connections between all QHINs? Which would have the benefit of enhancing ability to support failure of any one connection, but would introduce duplicate pathway problems. https://healthcaresecrecy.blogspot.com/2018/04/de-duplicating-received-duplicate-data.html
P. 21) QTF-003	This seems like a requirement inside a QHIN, which the first page of the QTF indicates is out of scope of this specification.
P. 22) QTF-004 ...TLS server certificates...	TLS certificates, not specifically only for servers. Clients need these to for mutual-authentication.

P. 22) QTF-004	I am expecting that the PKI requirements would be the primary policy that QTF would declare as it is the key to communications end-to-end.
P. 22) Secure Channel	Please leverage the ATNA secure channel specification. Reproducing the technical specifications here without re-using the IHE profile is not helpful to the reader. The named options in ATNA would be useful to evaluate and specify where they are important.
P. 22) Secure Channel	It is interesting that this section seems to be about encryption and integrity protecting (given the next section is on mutual-authentication; and yet this section does not specify any encryption or integrity protection settings.
P. 22) QTF-008	what is the justification for this requirement? Where does these details come from? What is the relationship of these requirements to BCP105 and/or IHE-ATNA?
P. 23) Mutual Server Authentication	Just Mutual Authentication. One can't mutually authenticate servers, as a client connects to a server. Servers do not connect to Servers.
P. 23) Mutual Server Authentication	Please leverage the ATNA secure channel specification. Reproducing the technical specifications here without re-using the IHE profile is not helpful to the reader. The named options in ATNA would be useful to evaluate and specify where they are important.
P., 23) Mutual Server Authentication	Given that this section is about authentication of the TLS, I would expect requirements to confirm the connections are authentic, chain to a trusted PKI root, using certificates for the purpose of TLS, using certificates that have not expired or are not revoked. All things that IHE-ATNA has specified.
P. 23) User Authentication	Note that the XUA assertion used in an HIE needs to be carefully intended and carefully interpreted. The Authenticating agent is the Organization initiating the transaction, that Organization will include the user who triggered the transaction. But the transaction is on behalf of the Organization. In that any results returned will be used by the Organization for the given PurposeOfUse(s); and is not limited to only the given triggering user. Often the trigger is not a user, but a workflow (e.g. a background task). Thus the XUA assertion should primarily be a statement of who the requesting Organization is, and the PurposeOfUse(s) that organization is going to use any data returned. The triggering user may be useful for audit logging, and may be used for access control (that is policy).
P. 24) QTF-014	This requirement is indicating that the QHIN must commit fraud. This solution is NOT acceptable, not technically or security. A counter-Signature may be appropriate; but replacing the signature is signing content that is not under the control. Anternative is that a new SAML is crafted on behalf of the QHIN leveraging the information in the intial.
P. 24) QTF-015	Why is PurposeOfUse(s) not mandatory? How is any responding agent going to be expected to expose data for no given purposeOfUse, that would be the equivilant of allowing the data to be used for any purposeOfUse.
P. 24) QTF-015	What about when the transaction is triggered by an automatic workflow, such as morning batch fetch? There would be no user in that case.
P. 24) Authorization & Exchange Purpose	Is this indicating that TWO saml assertions are required? Or is this referring to the PurposeOfUse element within the above specified XUA assertion.
P. 25) Table 7	What is the system for these codes? I would recommend that the HL7 purposeOfUse codes be used whenever possible. They are defined in far more detail than the codes defined here in Table 7.

P. 25) PurposeOfUse(s)	It is unclear, but seems indicated, that this specification is indicating that only one PurposeOfUse code will be used in any SAML assertion. This is inappropriate as the SAML should carry ALL of the purposeOfUse for which the data will be used. This would include for most treatment cases that the data will not just be used for treatment, but also payment and normal operations (aka TPO).
P. 25) Patient Discovery Query	How is this section related, or different to that which starts on Page 11?
P. 26) QTF-025	as in using ATNA and XUA? If so, then say that.
P. 26) QTF-***	These seem to be restating the normative requirements of XCPD. Do not replicate the normative requirements unless you are going to replicate ALL of the normative requirements... JUST DON'T replicate the normative requirements. Indicate they must be XCPD compliant.
P. 27) QTF-029	Note this is a requirement on the Directory lookup, that it can identify the HCID for any given Assigning Authority across the whole network of networks. And identify all the HCID across the whole network for broad lookup.
P. 27) QTF-030 ... capable of processing ...	what does "capable of processing" mean? is this referring to a food-processor? Note specific requirements already exist within XCPD and compliance to XCPD is all that should be stated here.
P. 27) QTF-031 ... capable of processing ...	what does "capable of processing" mean? is this referring to a food-processor? Note specific requirements already exist within XCPD and compliance to XCPD is all that should be stated here.
P. 27) QTF-032 ... capable of processing ...	what does "capable of processing" mean? is this referring to a food-processor? Note specific requirements already exist within XCPD and compliance to XCPD is all that should be stated here.
P. 27) QTF-033	This is a requirement on the internals of the initiating QHIN, which the first page of the QTF indicates is out-of-scope of the QTF. Untestable as stated.
P. 27) QTF-034	What is the justification for this https://profiles.ihe.net/ITI/TF/Volume2/ITI-55.html#3.55.4.2.2.5
P. 27) Patient Discovery Query	Note that an XCPD positive match always has some risk of false-positive. the absence of a match has some risk of false-negative. Thus the more matches you have, the more multiplication of the false-positive risk; and the potential responders that don't match multiply the false-negative risks.
P. 27) Document Query and Retrieve	What is the relationship to the above text and this text?
P., 27) IHE does not define a document beyond ...	IHE does define document content profiles. I think this statement is specifically about the Document Sharing transport implementation guides. edit: IHE Document Sharing Health Information Exchange does not define constrain a document beyond "
P. 27)	May be useful to insert here that FHIR-Documents vs simply FHIR resources. Although a document may be simply a single FHIR resource, a FHIR search set Bundle, or a FHIR document Bundle.
P. 27)	FHIR has a FHIR-Document covering the same use-case as C-CDA, the International Patient Summary (IPS). IHE has an IPS Profile that shows how the IPS document is carried in the Document Sharing infrastructures.
P. 27)	Note the whitepaper is updated and available at https://profiles.ihe.net/ITI/HIE-Whitepaper/index.html

	<p>P. 28) If a Responding Source is unable to return a C-CDA 2.1 document, the data is converted to the C-CDA 2.1 format by a Responding QHIN, Participant, or Subparticipant prior to transmission to the Initiating QHIN.</p>	<p>This is a unusual requirement. This would mean that where the source produces a TIFF only that somehow the QHIN must be able to produce a valid C-CDA out of that? This kind of conversion is NOT typical of XCA. XCA is content agnostic, and content preserving. Although best-case goal, this kind of a requirement will prevent useful source that can't produce structured and coded content.</p>
	<p>P. 27)</p>	<p>Many of these requirements are re-statements of XCA requirements, when XCA compliance should simply be required. Including duplicate requirements forces the reader to determine which requirements are not new. Only those requirements that are distinct from XCA requirements should be listed.</p>
	<p>P. 27) Document Query and Retrieve</p>	<p>Should indicate that FHIR-Documents are encouraged to be supported in addition to C-CDA documents that are required here. The HL7 IPS document is profiled for use in XCA by the IHE-IPS profile.</p>
	<p>P. 27) Document Query and Retrieve</p>	<p>When a document needs to be Digitally Signed. The use of the IHE-DSG profile must be used. https://profiles.ihe.net/ITI/TF/Volume1/ch-37.html This profile enables signatures across any kind of document including PDF, CDA, and FHIR. This profile enables the signature to be executed by a trust-framework PKI issued certificate. This signature purpose may be added to the QTF PKI certificate requirements. This digital signature specification does not hinder access to the document, as the signature is in a related DocumentEntry through a signs association. Thus being available when needed, but not introducing any barrier to access of the signed document.</p>
	<p>P. 27) Document Query and Retrieve</p>	<p>When a document is needing to be end-to-end encrypted, the IHE-DEN profile may be used. https://profiles.ihe.net/ITI/TF/Volume1/ch-32.html This profile encapsulates the document and blinds the metadata as appropriate for protecting the content. This profile can be used with PKI, but may be used with a shared key. This profile will encrypt any document type including PDF, CDA, and FHIR.</p>
	<p>P. 30) Message Delivery</p>	<p>How is this different than the above section on Message Delivery? (Why is this Message Delivery, Pushing would be more descriptive, or Content Delivery)</p>
	<p>P. 30) Message Delivery</p>	<p>Not clear that XCDR is necessary as XDR can work using Intended Recipient.</p>
	<p>P. 32) Patient Identity Resolution</p>	<p>Should there not be a mandatory minimum demographics required of requests? Can a responder fail to attempt a match if not given sufficient entries? What is the definition of demographics? Does demographics include identifiers, gender, address, phone numbers, etc?</p>
	<p>P. 32) Patient Identity Resolution</p>	<p>Note that an XCPD positive match always has some risk of false-positive. the absence of a match has some risk of false-negative. Thus the more matches you have, the more multiplication of the false-positive risk; and the potential responders that don't match multiply the false-negative risks.</p>
	<p>P. 32) Patient Identity Resolution</p>	<p>Note that a matching Assigning Authority and Home Community ID -- is an indication of Record Location. As in there are likely Records Here. Where XCA indicates what records are here. Or more specifically, what records are accessible.</p>
	<p>P. 32) Record Location -- This QTF Draft 2 does not specify a particular technology or standard for QHINs to use to locate patient records.</p>	<p>WHAT? It sure seems to indicate XCPD + XCA. What am I missing?</p>
	<p>P. 32) Record Location -- QTF-068 A Responding QHIN MUST be capable of identifying which, if any, of its Participants and/or Subparticipants are the Responding Source.</p>	<p>What does that mean? I have no idea how to parse that sentence, or how to apply it to the 32 pages of text above it.</p>

P. 32) Directory Services -- Directory services enable entities to manage information associated with healthcare organizations and persons.	why now using the word "persons"? edit - Directory services enable entities to manage information associated with healthcare organizations and personspractitioners .
P. 33) QTF-***	These requirements require a specific configuration of data within the directory to represent the relationships shown. What is the Implementation Guide (aka. Profile) used to express this relationship type?
P. 33) QTF-***	It seems many of these are requirements of each of the QHIN leads, not of the RCE.
P. 33) footnote 24	URL is undefined
P. 33) Auditing	I am expecting some Audit Log retention requirements? Is there some age at which audit log entries can be purged?
P. 33) Auditing	What is the requirement for audit log accessibility? Is the ATNA Audit Query transaction a recommendation or requirement?
P. 33) Auditing	What is the requirement for audit log use? Is there some policy?
P. 35) QTF-081	This is an infinite set. Is this really the requirement?
P. 35) QTF-082	I think you mean one identifier per Assigning Authority
P. 36) QTF-087	The ACP is identifying a policy, not a policy format. This is not the right use of this element. To learn of the format, one must query the documentEntry and look at the metadata returned. There are standards for this, what is specified here is not following standards.
P. 36) I)ACP Document contains access consent and is in XACML format	This is specifying the IHE-APPC format? If so, then use that profile.
P. 36) QTF-088	This is a statement of policy. It would be unusual for an initiating actor to demand this of a responding organization.
P. 36) (I)ACP	Pick one. there are two totally different concepts. ACP is a policy identifier, IACP is an instance of a signed consent by a specified patient. There is no such thing as a "(I)ACP"
P. 36) QTF-091	This is a statement of policy. The responding system should make this policy decision.
P. 36) QTF-093 and QTF-094	Why are these here? These are directory responsibilities.. that have already been made. remove these.
General	I think this model expressed in the QTF does use HCID always as the responding source, and does not mention/allow intermediaries that re-write HCID to be the HCID of the intermediary.
General	HCID is a custodian identifier, not a "next hop" identifier. Meaning that an HCID is independent of perspective. This means that an intermediary can't hide other HCID identifiable custodians behind itself thru re-writing the real custodian's HCID.
General	note the XCA audit event needs to recognize that one XCA transaction may have addressed multiple HCID... is that clear it is 1..*, or does the spec say 1..1?

	General	<p>rewriting saml assertions is a bad idea. Better to fall back on the very fact that the whole network is communicating sensitive health information reliant purely on the network of networks trust fabric as enforced by ATNA (TLS mutual-auth). Thus like the PHI that is communicated in this channel, the SAML information in this channel is trustable. thus there is no need for a special signature on the SAML, and thus at the ultimate destination there is no need to check a signature. The ultimate destination can just trust the saml attributes. If this can't be trusted, then how can the initiator trust the PHI that comes thru the very same TLS channels? Either the TLS/PKI is trustworthy or it is not.</p> <p>Yes it is understood that some networks do have an additional signature on the SAML within their network. I don't think this is necessary either, but the fact that it happens is not reason to force the network-of-networks to carry out this unnecessary signature creation or validation.</p>
--	---------	--