Appendix 3: The Sequoia Project: Detailed and Technical Comments – February 16, 2018

ONC DRAFT TRUSTED EXCHANGE FRAMEWORK

Published: January 5, 2018

Introduction and How Will It Work

Page	Section	Provisions	Comments
6		However, establishing a single "on ramp" to Electronic Health Information that works regardless of one's chosen network is feasible and achievable.	We understand the importance to providers of simplified access to exchange networks, and for interoperability to be highly usable and affordable. We strongly support simplified access to exchange networks and a single "on ramp" where feasible. At the same time, we are not certain that a single on ramp across *all* identified use cases and permitted purposes, is necessary or appropriate, or the most cost-effective option, when one considers certain specialized use cases (e.g., prescriptions) or emerging models, like API-based data access. We believe that ONC should permit specialized (e.g. by use case or technology) QHINs and ensure as well that Participants that have specialized missions can participate. Participants will work with QHINs that best meet their needs. Multiple on-ramps could in fact be less costly in some circumstances because they are tailored to a specific use case.
6		To that end, the Trusted Exchange Framework focuses on policies, procedures, and technical standards that build from existing HIN capabilities and enables them to work together to provide that single "on-ramp" to Electronic Health Information regardless of what health IT developer they	We agree with the intent to build on existing HIN capabilities and to enable exchange across technology platforms and networks. We are not certain, however that the draft TEF really builds on existing HIN capabilities. In particular, we are concerned that too few current or foreseeable organizations could meet the requirements to be a QHIN.

		use, health information exchange or network they contract with, or how far across the country the patients' records are located.	
6		At the same time, this "on-ramp" will still allow HINs to innovate and build out additional use cases and services that would provide value to their Participants and support their long-term sustainability.	We agree with the intent but are concerned that the focus on a single on ramp for all use cases, could hinder innovation or prescribe one particular architecture for all data exchange.
7		While we applaud the progress made to date and the hard work each organization has contributed to move the industry forward, additional and faster progress must be made; this is particularly true in the case of medical specialties—such as long-term services and supports (LTSS)[13] providing post-acute care or in lieu of institutionalization, behavioral health, and other ambulatory services. The Trusted Exchange Framework's minimum set of policies, procedures, and technical standards are intended to advance interoperability, particularly with these stakeholders, and enable them to use HINs to support the many use cases that are important to them and their patients (clients), including the exchange of data for Treatment, Payment, Health Care Operations (TPO)[14], Individual Access, Public Health,[15] and Benefits Determination.[16]	We agree with the need for more progress but also note that the lack of exchange in some sectors likely reflects the underlying lack of health IT adoption, for example in LTSS and behavioral health. In those areas where health IT and EHR penetration is high, we have seen significant levels of standards-based exchange. For Carequality and eHealth Exchange, see Appendix 2.
7		In an effort to develop and support a trusted exchange framework for trusted policies and practices and for a common agreement for the exchange between HINs, the proposed Trusted Exchange Framework supports four	Overall, we strongly support these capabilities while recognizing that additional R&D and further architectural and national-level implementation discussions must take place, especially in emerging areas like population level data exchange. Access to a standard, even a mature and well accepted standard, for example, is just one of the multiple building blocks needed to operationalize

		important outcomes: 1) providers can access health information about their patients, regardless of where the patient received care; 2) patients can access their health information electronically without any special effort; 3) providers and payer organizations accountable for managing benefits and the health of populations can receive necessary and appropriate information on a group of individuals without having to access one record at a time (Population Level Data),[17] which would allow them to analyze population health trends, outcomes, and costs; identify at-risk populations; and track progress on quality improvement initiatives; and 4) the health IT community has open and accessible application programming interfaces (APIs) to encourage entrepreneurial, user-focused innovation to make health information more accessible and to improve electronic health record (EHR) usability.[18]	this use case. We strongly recommend that ONC seek to catalyze (but not lead or define) prioritization and national-level implementation coordination. 1. We agree with this intent. 2. We also note that it will be important that the focus on "without special effort," while an element of Cures and desirable, be implemented in ways that are achievable and increasingly evolving, similar to the approach that ONC is taking with the proposed USCDI. 3. On the bulk query use case, we agree with and appreciate ONC's sensitivity to bandwidth and performance issues. 4. We agree with the emphasis on expanding API-based access but also urge ONC to recognize that for some HINs, this model may not be the most appropriate technology approach. We also encourage ONC to consider to what extent should the APIs themselves be standardized vs. developed using FHIR or a similar standard? We generally believe that the focus should be on APIs developed using standards vs. standardized APIs.
8		In addition, the Trusted Exchange Framework focuses on broadly applicable use cases that are discussed further below. The use cases identified are structured to address the areas of greatest need while also allowing existing HINs and trust frameworks to vary as appropriate to meet more specialized use cases that are specific to their own Participants.	We emphasize that TEFCA terms should be use case agnostic and reflect universal terms that apply to and can endure across multiple use cases.
8		We believe that this approach will significantly reduce the need for multiple point-to-point interfaces. As stakeholders noted during the public comment process,	The desire to reduce point-to-point interfaces is an appropriate goal but it also needs to take into account appropriate variation in HIN types and different use cases. Similarly, the intent to specify the minimum set of policies, procedures, and

		these interfaces are costly, complex to create and maintain, and an inefficient use of provider and health IT developer resources. It should be noted that while the Trusted Exchange Framework is structured to create a single "on-ramp" for the most common exchange use cases, it does not prevent organizations from creating point-to-point or one-off agreements between organizations who have a particular business need to exchange data in a manner that is different from the minimum set of policies, procedures, and technical standards outlined in the Trusted Exchange Framework, provided that such agreements do not undermine the policies of the Trusted Exchange Framework.[19]	technical standards to enable the use of that data for the broadest set of use cases makes sense in terms of "minimum necessary" but conflicts with the desire to focus on the broadest set of use cases possible.
8		To achieve the "on-ramp" ONC has identified, there are steps that must be taken to ensure that networks that are responsible for the flow of Electronic Health Information follow a minimum set of policies, procedures, and technical standards to enable the use of that data for the broadest set of use cases possible—the use cases that all stakeholders will benefit from. The provisions in the Trusted Exchange Framework are necessary for patient care, care coordination, and the overall health of the population and can only be successful with the participation of—for example—existing networks, health IT developers, and federal agencies.	

8		While we recognize that the provisions we have laid out in the Trusted Exchange Framework will necessitate modifications to existing participation agreements and trust frameworks to support provisions such as the additional permitted disclosures of health information by the Qualified HINs, we believe that these changes are necessary for us to meet the objectives identified by Congress and will enable providers and patients to have a single "on-ramp" to exchange.	The costs and benefits of such changes need to be considered by ONC as it evaluates comments and works with the RCE to finalize the TEFCA, as well as the time that will be needed for these changes to be made in existing agreements given the proven and hard-won governance process of existing HINs and prospective QHINs. We note that the draft TEF duplicates or covers the same ground in similar fashion in existing trusted exchange frameworks but does so in an overall structure that will require re-work by these networks.
9		This Draft Trusted Exchange Framework contains two parts: Part A – Principles for Trusted Exchange and Part B – Minimum Required Terms and Conditions for Trusted Exchange. Part A provides guard rails and general principles that Qualified HINs and HINs should follow to engender trust amongst Participants and End Users. Part B provides specific terms and conditions that will be incorporated into a single Common Agreement by a Recognized Coordinating Entity (RCE). Subsequently, ONC will publish on our public website and in the Federal Register the TEFCA, which is the combination of the Trusted Exchange Framework and the Common Agreement.	This overall approach seems reasonable. We suggest that ONC should permit continued use of existing common agreements that reflect the principles adopted under the TEFCA.
9		ONC intends to select through a competitive process a single RCE that will incorporate the Part B requirements into a single Common Agreement to which Qualified HINs may voluntarily agree to abide. The RCE will be tasked with operationalizing the Trusted	We agree with the designation of an RCE, which will bring private sector experience to the critical role envisioned by ONC. The entity that is selected to serve as the RCE should be organized and operated for the public interest and not a private benefit. The entity must have open and transparent governance that incorporates the perspectives of all relevant stakeholders. The RCE must be able

		Exchange Framework. We believe that a single, industry-based RCE is best positioned to operationalize the Trusted Exchange Framework. Implementing the TEFCA requires day-to-day management and oversight of unaffiliated Qualified HINs, including: onboarding organizations to the final TEFCA, ensuring Qualified HINs comply with the terms and conditions of the TEFCA, addressing non-conformities with Qualified HINs, developing additional use cases, updating the TEFCA over time, and working collaboratively with stakeholders. ONC intends to work closely with the RCE and to be continually involved in implementation of the TEFCA. We look forward to stakeholder comment on this approach. Because the RCE will be tasked with operationalizing the Trusted Exchange Framework, we have chosen in Part B to focus solely on provisions that are currently variable across HINs and that prevent the exchange of Electronic Health Information between HINs. Part B is not intended to be an all-encompassing participation agreement. To operationalize the Trusted Exchange Framework, the RCE will incorporate additional, necessary provisions into the Common Agreement as long as such provisions do not conflict with the Trusted Exchange Framework, as approved by ONC. The RCE will be expected to monitor	to ramp up quickly so that valuable time is not lost finalizing the TEF and developing the CA. Based on our experience as a convener of governmental and private sector stakeholder to advance interoperability, we have developed a list of criteria that we believe are essential to any organization that seeks to become the RCE. These criteria are included with our comments as Attachment 1. The expectations of the RCE should be clearly articulated to assure maximum transparency and engagement across stakeholders. This clarity is essential for the RCE to be effective in meeting the expectations and for all QHINs and HINs to clearly understand the scope of the RCE's authority and responsibility. It is also essential that the ONC role vis a vis the RCE be transparent and that ONC decisions that are regulatory and policy defining in nature provide for public notice and comment process. Overall, we believe that the RCE should have significant flexibility to bring forward private sector solutions that align with the ONC-specified goals. Given the stated ONC intention to leverage existing work, as indicated previously, we urge ONC to focus on specifying policy objectives and principles in a less detailed and prescriptive TEF. ONC should then work with the RCE, and other key stakeholders, to develop a common agreement that aligns with these principles and goals. ONC should seek to minimize the extent to which existing private sector organizations, whether RCE, QHINs or HINs need to retrofit existing agreements. We also suggest that ONC work with the RCE to ensure that RCE additions to the TEF as part of the Common Agreement are the minimally necessary additional provisions to implement ONC principals and goals, to minimize cost, complexity, disruption for HINs and their Participants and End Users. We note that the tasks assigned to the RCE are doable and have clear private sector precedent. For example, the Carequality framework already has mechanisms to: onboard, verify compliance, obtain executed copies of terms, have assurances of flow-downs, with mechanisms for dispute notification and resolution

		Qualified HINs compliance with the Common Agreement and take actions to address any nonconformity with the Common Agreement—including the removal of a Qualified HIN from the Common Agreement and subsequent reporting of its removal to ONC. The RCE will also be expected to work collaboratively with stakeholders from across the industry to build and implement new use cases that can use the TEFCA as their foundation, and appropriately update the TEFCA over time to account for new technologies, policies, and use cases. ONC believes that a private-sector organization would be best positioned to serve as the RCE and, to that end, we intend to release an open and competitive Funding Opportunity Announcement (FOA) in spring 2018 to award a single, multi-year Cooperative Agreement to an RCE. The multi-year Cooperative Agreement will allow ONC to closely collaborate with the RCE to help ensure that the final TEFCA supports all stakeholders and that interoperability continues to advance. In general, we believe the RCE will need to have experience with building multi-stakeholder collaborations and implementing governance principles. The FOA announcement will provide additional specificity on the eligibility criteria that an applicant would have to meet to be chosen as the RCE.	and breaches. The critical point to emphasize in final RCE design is the ability for the RCE to act as a neutral convener to assure that balanced interests are represented. To this end, we strongly encourage close coordination with the RCE and stakeholders with sufficient mechanisms for input and maintenance of the principles and terms.

10		The voluntary adoption by Qualified HINs of the Common Agreement may require that each network make upgrades to its health IT capabilities and align to certain trust and operational practices. Over time, and with the approval of ONC, the RCE will update the Common Agreement as necessary to account for new technical standards and policy requirements. ONC will work with the RCE to develop and/or implement a process for such updates.	It will be essential that ONC allow enough time for upgrades to agreements and technology capabilities. The anticipated upgrades are likely to be substantial in scope and cost. We note that the changes envisioned by ONC, especially to achieve the single on ramp, could lead to a convergence and duplication of capabilities that does not reflect the different missions and use cases of some QHINs and HINs. Overall, we believe that the update process should provide for less ONC direction than is suggested by this language, using a more collaborative approach, in which ONC is informing priorities, but with significant latitude to the RCE to coordinate implementation plans.
10		Qualified HINs that voluntarily adopt the final TEFCA will be included in ONC's online TEFCA directory, as directed by the Cures Act. If a Qualified HIN adopts the final TEFCA, is posted in the TEFCA directory, and subsequently decides not to continue participation in the TEFCA, ONC will remove the Qualified HIN from the online TEFCA directory.	We recognize that ONC must publish an online directory per Cures but suggest that it might meet this intent by pointing to a directory maintained by the RCE if that would meet Cures-related requirements.
11	Comment Process	Are there particular eligibility requirements for the Recognized Coordinating Entity (RCE) that ONC should consider when developing the Cooperative Agreement?	We propose the below RCE eligibility and operational requirements: **Corporate Structure and General Capabilities** • Legal entity capable of contracting with ONC; • Be established and operated for the public benefit as evidenced by 501(c)(3) tax-exempt status from the IRS as an organization that lessens the burden on government; • Can operationalize the TEFCA under current corporate and organizational structure (with feasible near-term revisions to structure as needed); • Organizational ability to "wall off" non-RCE exchange initiatives to avoid any conflicts of interests;

			• Financially stable; • Relevant experience and operational capability; and • Management and support infrastructure sufficient to manage the Cooperative Agreement. **Governance and Operations** • Governing body has authority to govern the RCE or establish an RCE governance structure; • Balanced stakeholder representation • Effective size and balanced composition given mission and tasks; • Formal, open and transparent governance and operational process; • Makes publicly available its governance structure and process, work products, policies, agreements, and pricing; • Active and ongoing stakeholder-focused engagement, communication, and education: (e.g. through regularly scheduled public calls, presentations and other avenues); • Publicized mechanisms for stakeholder and public input; and • Mechanism for dispute resolution. **Multi-Stakeholder Engagement with Balanced Representation** • Active engagement of both private sector (multiple stakeholders) and government (multiple agencies); and • Provides ability for diverse stakeholders to engage and have an active voice in the process for developing and maintaining policies, implementation resources and governance. **High Level of Relevant Experience and Outcomes** • Experience as a national convener of diverse stakeholders/collaborative to advance health information exchange and interoperability; • Experience working with federal agency partners, including under formal agreements; • Currently supports operational exchange via a trust framework and common agreement, including experience with query-based exchange;

			• Demonstrated track record with tasks required of the RCE, with outcome of such work in production at scale; and • Existing relationships with likely QHINs and Participants. **Ability to Act in a Fair and Neutral Manner** • Owners or members cannot require the entity to act in their best interests as opposed to the public good or otherwise unduly influence the RCE; • Is not invested in any specific technical architecture; • Able to be objective - may not advocate for specific industry stakeholder group(s) interests ○ Note: trade associations and similar organization are required by their mission to advocate for the interests of their members; • It is not under obligation to any technology vendor or type of system; • Has taken specific and enforceable steps to address conflicts of interests; and • Adopts a formal code of conduct for governing body members, staff and leaders.
11	Comment Process	Are there standards or technical requirements that ONC should specify for identity proofing and authentication, particularly of individuals?	ONC should recognize the identity proofing and electronic authentication requirements used in NIST 800-63 R3 https://pages.nist.gov/800-63-3/.
11	Comment Process	We recognize that important health data, such as that included in state Prescription Drug Monitoring Program (PDMPs), may reside outside of EHR/pharmacy systems. In such cases, standards-enabled integration between these systems may be necessary to advance, for example, interstate exchange and data completeness. As such, we invite comment on the following questions:	Overall, we applaud ONC for focusing on the opioid crisis and the role of PDMPs. Whatever model is chosen for the TEFCA should support a solution to this crisis. Certainly, we encourage exchange of PDMP data via the QHINs and other approaches to exchange, while again noting our earlier point that a *single uniform* on ramp model may not be fully appropriate for more specialized use cases. PDMPs and their supporting technology vendors should have the ability and be encouraged to function as HINs to exchange data through the TEFCA-organized exchange model.

11	Comment Process	How could a single "on ramp" to data that works regardless of a chosen HIN support broader uses for access and exchange of prescriptions for controlled substances contained in PDMPs?	
11	Comment Process	Given the variation of state laws governing PDMP use and data, should interstate connectivity for PDMP data be enabled via a TEFCA use case to address the national opioid epidemic?	
11	Comment Process	Is there an existing entity or entities positioned to support the opioid use case directly either as a Qualified HIN within the draft Trusted Exchange Framework or within the proposed Trusted Exchange Framework as a Participant of Qualified HINs? Is there an existing entity or entities positioned to support the opioid use case outside of the draft Trusted Exchange Framework? What is the readiness and feasibility of available standards to support the above and how have they been adopted to date?	
11	Comment Process	How could a TEFCA involved approach for supporting opioid use cases distinguish between technical capabilities versus applicable organizational, local, state, and/or federal requirements for PDMPs?	

11	Comment Process	When a federal agency's mission requires that it disseminate controlled unclassified information (CUI) to non-executive branch entities, but prohibits it from entering into a contractual arrangement, the agency is nevertheless directed to seek the entity's protection of CUI in accordance with Executive Order 13556, Controlled Unclassified Information, or any successor order, and the CUI Program regulations, which include requirements to comply with NIST SP 800-171. How best should TEFCA address these requirements?	This is an important issue and should be addressed as part of ONC and RCE work with other federal agencies and private stakeholders. It's likely that compliance with NIST SP 800-171 requirements will present operational challenges, particularly for small organizations. Even for organizations with sophisticated information technology infrastructure, current security practices may not align perfectly with the CUI Program regulations. We believe it is operationally impractical to impose these requirements on the entire TEFCA ecosystem, and propose that the TEFCA be silent on this issue.

Part A – Principles for Trusted Exchange

Page	Section	Provisions	Comments
13	Purpose and Scope	Part A of the TEFCA provides a set of core principles by which Qualified HINs—as well as all HINs—and data sharing arrangements for data exchange should abide. Specifically, these principles support the ability of stakeholders to access, exchange, and use relevant Electronic Health Information across disparate networks and sharing arrangements. Part B aligns to and builds from these principles to address a minimum set of terms and conditions to enable network-to-network exchange of Electronic Health Information.	We believe that detailed normative language should only be in Part B. The mix of principles and detailed normative language in Part A adds confusion, especially with respect to its relevance to Part B.
14	Principles	Principle 1 - Standardization: Adhere to industry and federally recognized technical standards, policies, best practices, and procedures.	We agree with this principle.
14	Principles	A. Adhere to standards for Electronic Health Information and interoperability that have been adopted by the Secretary of the U.S. Department of Health & Human Services (HHS) or identified by ONC in the Interoperability Standards Advisory (ISA).23	The focus on adoption is appropriate but the TEFCA should rely, as indicated, on detailed implementation guides for standards specification rather than including these specific requirements in the body of the legal agreement. These guides should take into account the maturity, suitability, and market readiness of specific standards (including the availability of implementation guides) adopted by the Secretary or included in the ISA. In addition, it is not clear that the ISA was designed or is appropriate for this purpose
14-15	Principles	Qualified HINs and their participants should adhere to federally adopted or recognized standards for Electronic Health Information and interoperability wherever possible, e.g. use	In general, we agree but please see our above comments. Again, it is not clear that either ONC 2015 certification or the ISA was developed with the TEFCA use case in mind. The 2015 edition was designed for use by EHRs and similar HIT and it is not

		of the Consolidated Clinical Data Architecture (C-CDA). Specifically, Qualified HINs should first look to use standards adopted or recognized through ONC's Health IT Certification Program (Certification Program) and in the ISA. If the Certification Program or the ISA do not have applicable standards, Qualified HINs should then consider voluntary consensus or industry standards that are readily available to all stakeholders, thereby supporting robust and widespread adoption. To that end, “proprietary” standards—that is, standards that incorporate or require the use of patented technologies or other intellectual property (IP)—should be avoided unless adequate commitments have been made to license all standards-essential IP pursuant to Reasonable and Non-Discriminatory (RAND) terms.[24] As new standards are adopted by HHS or recognized by ONC, Qualified HINs must implement the updated standards in a timely manner and work with the RCE to update the TEFCA with newer versions of standards as applicable. In 2015, the Secretary of HHS issued the 2015 Edition Health IT Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications final rule (2015 Edition final rule). [25] The 2015 Edition certification criteria (2015 Edition) help facilitate greater interoperability for several purposes and enables Electronic Health Information exchange	clear that it is defined in ways that are always directly applicable to HINs. Note also that the 2015 edition does not have an API standard per se (e.g., FHIR). Certainly, selection and requirements for use of standards should take into account not just applicability but also the maturity, suitability, and market readiness of specific standards (including the availability of implementation guides). On the issue of “proprietary” standards, it would be helpful for ONC to address how this provision applies to existing industry standards, including those adopted or recognized by ONC or incorporated in HIPAA transactions. We ask ONC to clarify the obligation of the RCE to update the TEFCA for new standards and can or must QHINs adopt the new or revised standards in advance of the formal TEFCA update? As indicated in other places in this comment, in our experience, it is more efficient to operate under a master legal agreement, with terms that do not change, and with implementation-level details in referenced implementation guides, policy documents, etc.

		through new and enhanced certification criteria, standards, implementation specifications, and Certification Program policies. The 2015 Edition incorporates changes that are designed to spur innovation, open new market opportunities, and provide more choices to stakeholders when it comes to Electronic Health Information exchange. For example, the 2015 Edition addresses a number of functionality needs related to care delivery, such as the capture of patient information, unique device identifiers for implantable devices, data transport mechanisms, and care plan data. The 2015 Edition also addresses a variety of data exchange flow patterns, including sharing patient data between providers and other health care organizations, between providers and patients, and between providers and public health departments. In addition to the 2015 Edition, ONC has released a Certification Companion Guide[26] for each criterion that further clarifies the certification criteria requirements. Certification enables End Users to have confidence that their health IT will support interoperability for the appropriate use cases and helps enable the exchange of Electronic Health Information in a structured way. Participants of Qualified HINs that provide services and functionality to providers should follow the 2015 Edition final rule and associated guidance for the certification of health IT	

		where applicable. Further, Qualified HINs that facilitate the exchange of health information should use the standards identified in the 2015 Edition final rule when appropriate for the use case to facilitate connections with other HINs. As noted above and in addition to the 2015 Edition final rule, the ISA is another resource for standards and implementation specifications. The ISA is a non-regulatory document that coordinates the identification, assessment, and public awareness of interoperability standards and implementation specifications that the industry can use to meet specific clinical health IT interoperability needs. The ISA includes informative characteristics about each standard and implementation specification, including, for example, a rating of standards process maturity (final or balloted draft) and information on implementation maturity (production or pilot). At a minimum, Qualified HINs connecting to other Qualified HINs should adopt and use standards and implementation specifications that are referenced in the 2015 Edition final rule and the ISA. Further, Qualified HINs should actively engage with ONC to improve and update the ISA's detail, in order to inform the content of the ISA and ensure that the appropriate and best standards are referenced for needed use cases.	

14	Principles	On IP issues, [24] See generally, Mark A. Lemley & Carl Shapiro, *A Simple Approach to Setting Reasonable Royalties for Standard-Essential Patents*, Stanford Public Law Working Paper No. 2243026 (November 5, 2013), *available at* http://ssrn.com/abstract=2243026 and http://dx.doi.org/10.2139/ssrn.2243026.	
14	Principles	[25] Under HIPAA, HHS adopted certain standard transactions for the electronic exchange of health care data. These transactions include: Claims and encounter information, Payment and remittance advice, Claims status, Eligibility, Enrollment and disenrollment, Referrals and authorizations; Coordination of benefits, and Premium payment and any of these transactions electronically must use an adopted standard from ASC X12N or NCPDP (for certain pharmacy transactions). The Administrative Simplification provisions under HIPAA and ACA falls under HHS and is carried out by the Division of National Standards (DNS) at CMS and do not apply here. ONC does not have jurisdiction over the standard transactions	We note that certain HIPAA transaction code sets (e.g., ICD-10) are also referenced in certification and the ISA.

		nor do we advocate any change in these transactions.	
15	Principles	B. Implement technology in a manner that makes it easy to use and that allows others to connect to data sources, innovate, and use data to support better, more person-centered care, smarter spending, and healthier people.	We agree with this principle.
15-16	Principles	Qualified HINs should use standards-based technology for exchanging Electronic Health Information with other Qualified HINs. Such technology should be implemented in accordance with standards and, as consistently as possible, follow implementation guides and authoritative best practices published by the applicable standards development organization (SDO). Minimizing variation in how standards are implemented will make it easier for others to connect to Electronic Health Information. Further, to the extent possible, Electronic Health Information stored in health IT products should be structured and coded using standardized vocabularies. Qualified HINs and their participants should provide accurate translation and adapter services to their End Users to enable them to map proprietary data to standard, user friendly vocabularies. Adapter services are designed to transform message content or, in this context, transform unstructured data to structured and coded vocabularies, so that	We agree but note that enforcement and maintenance will be a challenge. An RCE experienced in handling such issues will be essential. We question whether mapping and translation services are related to core principles for exchange between networks and suggest that functional and architectural requirements not be specified in Part A. We suggest reframing the policy objectives and leaving the mechanics silent in the principles.

		Qualified HINs can exchange data with other Qualified HINs in a standardized format. Qualified HINs should ensure that the data exchanged within their own network and with other Qualified HINs meets minimum quality standards by using testing and onboarding programs to verify minimum quality levels. Qualified HINs may consider using open source tools, such as ONC's C-CDA scorecard tool for testing the quality of C-CDAs.[27] They may also consider developing tools to test the quality of data exchange using Fast Healthcare Interoperability Resources (FHIR) APIs. These types of testing programs can help ensure that high quality data is exchanged both within and across HINs.	Note, these tools only evaluate certain aspects of data quality. We believe that ONC should be focused and realistic in terms of the data quality issues that can be made the responsibility of QHINs or HINs.
16	Principles	Principle 2 - Transparency: Conduct all exchange openly and transparently.	We agree with this principle.
16	Principles	A. Make terms, conditions, and contractual agreements that govern the exchange of Electronic Health Information easily and publicly available.	We agree.
16	Principles	All parties desiring to participate in Electronic Health Information exchange should know, prior to engaging with a Qualified HIN, the responsibilities of being a participant in a Qualified HIN, the responsibilities of acting as a Qualified HIN, and the protections that have been put in place to ensure that all privacy and security requirements are followed. Qualified HINs should voluntarily make these and other terms and conditions for participating in	We agree.

		their network easily and publicly available via their website; meaning they are not accessible only to members but also to the general public.	
16	Principles	B. Specify and have all participants agree to the permitted purposes for using or disclosing ePHI or other Electronic Health Information.	In our experience, specification of the permitted purposes should establish parameters around use and disclosure or the purposes for which data may be exchange between QHINs.
16-17		Since Qualified HINs are often either Business Associates for Covered Entities or for other Business Associates, their participation agreements specify the permitted purposes for which their network may be used to exchange data. While some Qualified HINs currently support all of the HIPAA permitted purposes, others may only support the Treatment permitted purpose. When Qualified HINs have varying, allowable permitted purposes in their own participation agreements, exchange between those Qualified HINs is limited and may not occur. This could prevent End Users from having a single "on-ramp" to interoperability. Consequently, Part B specifies a minimum set of Permitted Purposes that Qualified HINs and their participants and End Users must support. Qualified HINs may want to support additional permitted purposes and use cases for their participants. If so, they should clearly specify both the minimum set of permitted purposes that are supported and any additional permitted purposes for using or disclosing Electronic Health Information. These should be specified in the Qualified	We much agree that having a broad set of Permitted Purposes is desirable. We also recognize that enforcing mandatory participation in all permitted purposes may be a barrier to adoption of the TEFCA and of QHIN participation. Further, some specialized participants – such as public health agencies or those requesting records for benefits determination – would appropriately engage in exchange for only a single permitted purpose.

		HIN's legal agreement with Participants, made open and transparent consistent with Principle 2.A, and clearly communicated when Electronic Health Information is requested or sent between Participants and Qualified HINs.	
17	Principles	C. Publish, keep current, and make publicly available the Qualified HIN's privacy practices.	We agree.
17	Principles	HINs and their participants should ascribe to the following privacy practices: 1. Qualified HINs must comply with all Applicable Laws regarding the use and disclosure of ePHI or other Electronic Health Information. 2. Clearly specify the minimum set of "permitted purposes" for using or disclosing ePHI or other identifiable Electronic Health Information within the TEFCA and promote limiting the use of identifiable Electronic Health Information to the minimum amount required for non-treatment purposes. If there are technical variables, the Qualified HINs should clearly specify them. 3. Qualified HINs must have the capability to document and/or capture patient consent or written authorization if required by law and communicate such consent upon request.	We agree that HINs and participants should agree to specific privacy practices. We also agree that the specification of permitted purposes should describe the purposes for which data are exchanged, as well as what parties to the TEFCA and its flow-down agreements can do with the data. Practice # 3: The responsibility to obtain consent or authorization should remain with the organizations that are the sources of ePHI being released, and which have a relationship with the patient to make consent management feasible. QHINs may play a role in conveying patient preferences or consent decisions to facilitate information sharing, but should not themselves be required to document or capture consent. Practice #4: In addition to not impeding access, which is reasonable, do QHINs have an affirmative obligation to facilitate a patient's desire to direct his or her ePHI to a third party? If so, there may be operational issues due to the fact that the standards and approaches outlined in the TEF don't provide a well-defined mechanism for a push of information to a third party. Practice # 5: We believe that consent management is not a QHIN role but rather one for Participants and End Users. See our comment on Practice #3 above.

		4. Qualified HINs must not impede the ability of patients to access and direct their own Electronic Health Information to designated third parties as required by HIPAA. 5. Qualified HINs must have policies and procedures to allow a patient to withdrawal or revoke his or her participation in the exchange of his or her Electronic Health Information on a prospective basis. These privacy practices are critical to effective exchange and have been incorporated into the terms and conditions in Part B. To further promote transparency, providing public and written notice describing how health information will be used is incorporated into Part B. HIPAA requires that all Covered Entities provide to their patients a Notice of Privacy Practices (NPP). The draft Trusted Exchange Framework requires a participating Covered Entity that is a Qualified HIN to add this information to its existing NPP. The draft Trusted Exchange Framework requires a Qualified HIN that is not a Covered Entity to publish and make available a notice as well.	
17	Principles	Principle 3 - Cooperation and Non-Discrimination: Collaborate with stakeholders across the continuum of care to exchange Electronic Health Information, even when a stakeholder may be a business competitor.	We agree with this Principle, which aligns with one of the foundational principles of the Carequality Framework.

17	Principles	A. Do not seek to gain competitive advantage by limiting access to individuals' Electronic Health Information.	We agree with this principle.
17-18	Principles	Qualified HINs and their participants should not treat individuals' Electronic Health Information as an asset that can be restricted in order to obtain or maintain competitive advantage. For example, Qualified HINs and their Participants should not withhold health information requested for TPO purposes from healthcare providers or health plans that are outside of their preferred referral networks or outside of a value-based payment arrangement, such as by establishing internal policies and procedures that use privacy laws or regulations as a pretext for not sharing health information. Likewise, Covered Entities should not implement technology in a manner that permits limiting the sharing of data. Qualified HINs and their participants should practice data reciprocity (e.g., have a willingness to share Electronic Health Information themselves as opposed to only participating in an exchange relationship only for the purpose of receiving health information from others). In addition, Fees and other costs should be reasonable and should not be used to interfere with, prevent, or materially discourage the access, exchange, or use of Electronic Health Information within a Qualified HIN or between Qualified HINs. Part B further	We strongly agree with the principle that an individual's EHI should not be treated as an asset to be leveraged by Qualified HINs or their Participants. We do note that the details of this principle could be subject to interpretation and dispute. It will be important for the final CA and any accompanying implementation guides to provide clarity. We recommend that the TEF focus on practices being evenly applied in a non-discriminatory manner, rather than create a detailed list of prohibited behaviors. This approach will enable the TEF to remain durable as the eco-system evolves. We generally agree on reciprocity but it should be clear that a participant could act as a responder only and not as a source of queries.

		specifies requirements on making any such Fees between Qualified HINs reasonable. While Qualified HINs must comply with Applicable Laws, including the applicable HIPAA Rules – see OCR's guidance on the HIPAA Security Rule – they should not use contract provisions or proprietary technology implementations to unduly limit connectivity with other Qualified HINs, such as by preventing the appropriate flow of health information across technological, geographic, or organizational boundaries for health and care, safety, quality measurement, payment, or research as permitted by law. Qualified HIN participants must not prevent the sharing of Electronic Health Information for the permitted purposes specified in Part B because the receiving Covered Entity is considered a competitor. Additionally, Qualified HIN participants may not prevent the sharing of Electronic Health Information for such permitted purposes with a Covered Entity that is not in their preferred referral network or that is not part of an alternative payment model with the Qualified HIN Participant. Qualified HINs may not use methods that discourage or impede appropriate health information exchange, such as throttling the speed with which data is exchanged, limiting the data elements that are exchanged with healthcare organizations that may be their competitor or a competitor of one of their Participants, or requiring burdensome	We note that standards for fees will be difficult to establish or enforce but agree that fees should not be used with intent to restrict access. We agree in principle but "unduly" requires definition. This provision mixes intent and effect and will be challenging to define or enforce. What if "throttling" is non-discriminatory in intent and intended to manage resource use and bandwidth, even if it disproportionately affects some users?

		testing requirements in order to connect and share data with another Qualified HIN.	
18	Principles	Principle 4 – Privacy, Security, and Safety: Exchange Electronic Health Information securely and in a manner that promotes patient safety and ensures data integrity.	We agree with this principle.
18	Principles	A. Ensure that Electronic Health Information is exchanged and used in a manner that promotes patient safety, including consistently and accurately matching Electronic Health Information to an individual.	We agree that EHI should be exchanged and used to promote patient safety. There is the potential that requiring QHINs to "ensure" consistent and accurate matching will create a level of liability that will discourage organizations from becoming QHINs. Instead, we recommend that QHINs commit to support best practices for improving patient matching among its HINs and Participants. ,
18-19	Principles	Ensuring the integrity of electronically exchanged data is paramount to patient safety. When Electronic Health Information is exchanged, the promotion of patient safety begins with correctly matching the data to an individual so that care is provided to the right individual based on the right information. Sophisticated algorithms that use demographic data for matching are the primary method for connecting data to an individual. For example, for purposes of a health IT product seeking certification to the transitions of care criterion of the 2015 Edition, §170.315(b)(1) provides that when Electronic Health Information is exchanged in a C-CDA, a core set of patient demographic data must be included in a standardized format.[28] Likewise, Qualified HIN participants should ensure that the core set of	We ask that ONC clarify the responsibility of a QHIN participant in ensuring the presence of these core data elements; for example, would an HIN or a QHIN be responsible for ensuring that demographic data elements are included in C-CDAs that are accessed via queries. Such responsibility for data elements that originate with providers is not the norm today. The core set of demographic criteria to be captured should include data elements and associated metadata, determined by a consensus-based private-sector organization. Such criteria should specify data that can be used by patient matching industry standards such as the HL7 FHIR Patient resource and IHE XCPD (Cross-Community Patient Discovery). Furthermore, such requirements should specify pediatric demographics (which are rarely exchanged today). Finally, the ONC should allow for innovation, such as the use of emails, telephone numbers, palm vein scans, matching of people with housing instability, pre-natal patient matching, etc. We question the practicality of the proposal that QHIN participants "need to update individuals' clinical records to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another healthcare organization". We agree with the intent of providing up to date information, but a Participant is not necessarily an End User, and may not be in a position to update records. Even

		demographic data is consistently captured for all patients so that it can be exchanged in a standard format and used to accurately match patient data. In addition to the importance of the integrity of demographic data elements, overall Electronic Health Information integrity is a key component of promoting patient safety in electronic exchange. Where possible, standard nomenclatures should be used and be exchanged in a data format that is consumable by a receiving system, such as the C-CDA or via FHIR Application Programming Interfaces (APIs). Further, Qualified HIN participants need to update individuals' clinical records to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another healthcare organization. Finally, Qualified HINs and their participants should work collaboratively with standards development organizations (SDOs), health systems, and providers to ensure that standards, such as the C-CDA, are implemented in such a way that when Electronic Health Information is exchanged it can be received and accurately rendered by the receiving healthcare organization.	at the End User level, data could be provided in good faith as the most up-to-date information held by the sender, when in fact the patient has had more recent care – potentially years of more recent care - elsewhere. Further, this requirement would insert the QHIN into its Participants' and End Users' medical records practices and clinical workflows, which we believe is not an appropriate role for a QHIN. We agree that it's important for the implementation community to share experiences in order to continually improve standards implementation.
19	Principles	B. Ensure providers and organizations participating in exchange have confidence that the appropriate consent or written authorization was captured, if and when it is needed, prior	We agree.

		to the exchange of Electronic Health Information.	
19	Principles	The HIPAA Rules do not have a consent requirement for exchanging ePHI for Treatment, Payment, and most Health Care Operations purposes; however, the law does require an authorization from the patient to share ePHI for Health Care Operations purposes with another Covered Entity that does not have a relationship with the patient. Some state and federal laws do require patient consent for exchange of Electronic Health Information. For example, for some health conditions such as HIV, mental health, or genetic testing, state laws generally impose a higher privacy standard (e.g., requiring patient consent from the individual) than HIPAA. Additionally, under 42 C.F.R. Part 2, subject to certain exceptions, federally assisted "Part 2 programs" are required to obtain consent to disclose or re-disclose health information related to substance use disorder information, such as treatment for addiction. When required by federal or state law, a Qualified HIN's ability to appropriately and electronically capture a patients' permission to exchange or use their Electronic Health Information will engender trust amongst other Qualified HINs seeking to exchange with that network. For this reason, we have included this requirement in Part B.	We agree with the need to honor consent requirements where required by law; however, we question whether this should be the responsibility of the QHIN (which may be one or two steps removed from a patient relationship) to assure consent was obtained.
19	Principles	Principle 5 - Access: Ensure that Individuals and their authorized caregivers have easy	

		access to their Electronic Health Information.	We agree with the intent to support an individual's right of access to their information. We do propose, however, that a QHIN's role is to enable access, rather than ensure access.
19	Principles	Do not impede or put in place any unnecessary barriers to the ability of patients to access and direct their Electronic Health Information to designated third parties	We agree that unnecessary barriers should be discouraged. We propose, however, that the ability to access be considered distinct from the ability to direct. The latter, as noted above, is not actually supported by the standards and methods outlined in Part B. Aligning the TEF with forthcoming rules on information blocking should provide an opportunity for clarity on this point.
19-20	Principles	Stakeholders who maintain Electronic Health Information should (1) enable individuals to easily and conveniently access their Electronic Health Information, (2) be able to direct it to any desired location, and (3) ensure that individuals have a way to learn how their information is shared and used. This principle is consistent with the HIPAA Privacy Rule, which requires Covered Entities to provide PHI to patients in the form and format in which they request it, if it is readily producible in that form and format. This means that if it is stored electronically, patients can request it and access it electronically. HIPAA also requires Covered Entities and Business Associates to send PHI to a third party of the patient or authorized representative's choosing, upon request. Covered Entities and Business Associates may not impose limitations through internal policies and procedures that unduly burden the patient's right to get a copy or to direct a copy of their health information to a third	We agree with this principle, but note as above that the ability to direct information to a specified third party is generally outside of the scope of the messaging standards and operational approach envisioned by the specific Part B terms. Also, we are not certain that training requirements really should be defined by ONC materials. We agree with the importance of fostering openness and transparency, and that QHINs should provide reasonable opportunities for individuals to review information on who has retrieved their records.

		party of their choosing.[29] Likewise, Qualified HINs and their participants – most of whom are Covered Entities or Business Associates – should not limit third-party applications from accessing individuals’ Electronic Health Information via an API when the application complies with Trusted Exchange Framework requirements and is directed by the individual. In addition, Qualified HINs and their Participants should commit to training all staff members on helping individuals obtain electronic access as demonstrated by ONC’s access videos and infographic. Much like individuals’ access to their health information as required by HIPAA is important, it also is important for individuals to have access to information about who else has accessed or used their health information. As the Fair Information Practice Principles (FIPPs) of the Nationwide Privacy and Security Framework on openness and transparency states, “[p]ersons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format.”[30] HINs should commit to following this principle, and should provide such opportunities electronically whenever possible, particularly when an individual makes the request electronically. NPP can also	

		serve to help individuals understand how and when their health information is shared.	
20	Principles	B. Have policies and procedures in place to allow a patient to withdraw or revoke his or her participation in the Qualified HIN	The responsibility to obtain consent or authorization should remain with the organizations that are the sources of ePHI being released, and which have a relationship with the patient to make consent management feasible. QHINs may play a role in conveying patient preferences or consent decisions to facilitate information sharing, but should not themselves be required to document or capture consent
20		Some individuals may prefer not to have their health information electronically shared via a Qualified HIN. Consequently, Qualified HINs and/or their participants must maintain policies and procedures that allow a patient to revoke his/her participation in the Qualified HIN on a prospective basis. Such policies and procedures must be easily and publicly available and be consistent with the HIPAA Privacy Rule right of an individual to request restriction of uses and disclosures, and the process for revoking participation must be easily accomplished by patients.	See prior comment.
21	Principles	Principle 6 - Data-driven Accountability: Exchange multiple records for a cohort of patients at one time in accordance with Applicable Law to enable identification and trending of data to lower the cost of care and improve the health of the population.	We understand the importance of supporting data exchange, "to enable identification and trending of data to lower the cost of care and improve the health of the population." The specifics of how this is accomplished, however, should be addressed as a separate use case, subject to prioritization by a broad array of private and public sector stakeholders.
21	Principles	A. Enable participants to request and receive multiple patient records, based on a patient panel, at one time.	Please see our above comments.

21	Principles	Health systems and providers may want to use Qualified HINs to decrease the number of discreet interfaces they have to build to exchange Electronic Health Information with other Covered Entities or with their own Business Associates for TPO, Individual Access, Benefits Determination, and Public Health purposes. For example, a provider may want to use a Qualified HIN to share Electronic Health Information from their EHR to a qualified clinical data registry (QCDR), a qualified entity (QE), a health information exchange (HIE), or a health IT developer providing care coordination or quality measurement services. Payers and health plans, including employer sponsored group health plans may wish to work with Qualified HINs to connect to Electronic Health Information that would better support payment and operations, including using analytics for services such as assessing individuals' risk, population health analysis, and quality and cost analysis. These Population Level requests are fundamental to providing institutional accountability for healthcare systems across the country. Additionally, caregivers who are authorized legal representatives, known as "personal representatives" under HIPAA, may wish to access all of their family's records at one time, rather than having to request one record at a time for each family member to the extent permitted by law.	

		Supporting these types of use cases necessitates the ability to exchange multiple patient records at one time (i.e. population level or “bulk transfer”), rather than potentially performing hundreds of data pulls or pushes for a panel of patients. Qualified HINs should provide the ability for participants to both pull and push population level records in a single transaction. This decreases the amount of time a clinician’s resources are devoted to such activity and makes more time available for actual patient care.	Please see our above comment. Also note that the ability to push population level records is not only a distinct use case, but is also generally outside of the scope of the query-based messaging standards and operational approach envisioned by the specific Part B terms.

Part B – Minimum Required Terms and Conditions for Trusted Exchange

Page	Section	Provisions	Comments
22	Overview	As noted, Congress has charged ONC[32] with ensuring full network-to-network exchange of Electronic Health Information (EHI) through a trusted exchange framework and common agreement (TEFCA). In Part B, we seek to provide a set of minimum, required terms and conditions for the purpose of ensuring that common practices are in place and required of all participants who participate in the final TEFCA. We recognize that all Covered Entities and Business Associates are required to have existing Business Associates' Agreements applicable to the Uses and Disclosures of EHI. The following terms and conditions for trusted exchange align with all the requirements of and sit on the foundation of the HIPAA Rules. These terms and conditions are designed to help ensure, for example: • Common authentication processes of trusted health information network participants, • A common set of rules for trusted exchange, and • A minimum core set of organizational and operational policies to enable the exchange of EHI among networks. These terms and conditions will be reflected in the Common Agreement and	

		complement the principles and objectives contained in the Principles of Trusted Exchange (Part A). Together Part A and Part B are designed to enable all stakeholders to have a single "on-ramp" to electronic exchange of health information, ultimately easing provider and patient burden.	
23	Definitions	2015 Edition: the 2015 Edition certification criteria adopted at 45 C.F.R. 170.315. AALs: the Authentication Assurance Levels described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017). Applicable Law: all applicable federal or state laws and regulations then in effect. Application Programing Interfaces (API): a set of software instructions and standards that allows machine to machine communication. Attributable Cost: the Reasonable Allowable Cost of the Attributable Services. Attributable Services refers to both: (a) the services provided by a Qualified HIN that are necessary for the Qualified HIN to perform its obligations under the Common Agreement to the extent that the Qualified HIN is not providing such services prior to execution of the Common Agreement; and	We are not certain that this is the best or most apt API definition for TEFCA purposes. We suggest that the following excerpt from Wikipedia may better reflect ONC's intent. ONC may also wish to bind the definition of API in this document by focusing on or indicating its intended use. https://en.wikipedia.org/wiki/Application_programming_interface "In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components." It appears that QHINs would only be able to charge other QHINs for incremental services associated with the TEFCA but they should also be in a position to

		(b) the services and licenses (if any) that the Qualified HIN must obtain from a third party in order to enter into the Common Agreement and satisfy its obligations thereunder but only to the extent that such third party services and licenses are not already being used in the Qualified HIN's operations prior to entering into the Common Agreement. Without limitation of the foregoing, Attributable Services include: (i) the development or modification of APIs for future versions of the USCDI (to the extent that such APIs do not exist prior to execution of the Common Agreement); (ii) development of or revisions to the Broker in order to satisfy provisions of the Common Agreement that the Qualified HIN's Broker does not satisfy prior to entering into the Common Agreement; and (iii) the legal services necessary to enter into the Common Agreement and to amend the Qualified HIN's agreements with its Participants in order to meet the requirements of the Common Agreement.	charge QHINs for services that they provide that are pertinent to but predate the TEFCA. We suggest that ONC clarify that charges to other QHINs for services that predate execution of the CA are also permissible if they relate to the QHIN's responsibilities under the CA. We question whether this model could require QHINs to have very complex dual cost and pricing models.

		ATNA Integration Profile: the Audit Trail and Node Authentication Integration Profile that is part of the Integrating the Healthcare Enterprise (IHE) International IT Infrastructure Technical Framework. Benefits Determination: a determination made by any federal or state agency that an individual qualifies for federal or state benefits for any purpose other than healthcare (for example, Social Security disability benefits). Breach: has the meaning assigned to it in 45 C.F.R. §164.402 of the HIPAA Rules. Broadcast Query: an electronic method of requesting EHI (sometimes referred to as a "pull") that asks all Qualified HINs and their Participants and End Users if they have EHI of an individual or set of individuals rather than asking specific Qualified HINs and their Participants and End Users if they have EHI of an individual or a set of individuals.	
24	Definitions	Broker: see definition of Connectivity Broker below. Brokered Broadcast Query: a Broadcast Query that (a) uses a Record Locator Service to identify all locations in the Qualified HIN's network (including its Participants and their End Users) that hold an individual's EHI, (b) queries all such locations simultaneously, (c) retrieves all of the individual's EHI from such	

		locations and (d) transmits it back or makes it available to the person or entity that initiated the query. For example, and without limitation of the foregoing, a Broadcast Query that asks for only limited EHI about an individual (such as individual EHI only in certain zip codes) is not a Brokered Broadcast Query unless the limitation was imposed by the person or entity that initiated the Broadcast Query. Business Associate: has the meaning assigned to such term at 45 C.F.R. §160.103 of the HIPAA Rules. Common Agreement: the Standard Agreement of the RCE which either (a) initially includes these terms and conditions, or (b) if the RCE has a Standard Agreement prior to the publication of these terms and conditions, its Standard Agreement as modified to include these terms and conditions. The Common Agreement may include such terms from the Standard Agreement or other terms as the RCE and the Qualified HINs deem appropriate; provided, however, that in the event of any conflict or inconsistency between or among Applicable Law, these terms and conditions, the Standard Agreement or any other terms, the following shall be the order of precedence to the extent that there is any conflict or inconsistency: (i) Applicable Law including the HIPAA Rules, (ii) these terms and conditions, (iii) the Standard Agreement, and (iv) any	We appreciate that ONC recognizes that the RCE may have a predating standard agreement and that this standard agreement could be the basis for the Common Agreement as modified to reflect the final TEF. In addition, we believe that the role of the TEF principles and terms is to provide guidance for the development of the Common Agreement, and that they should not have precedence over the Common Agreement. We suggest that “ii” be deleted.

		other terms and conditions agreed to by the parties.	
		Connectivity Broker (Broker): a service provided by a Qualified HIN that provides all of the following functions as further described in these terms and conditions with respect to all Permitted Purposes: master patient index (federated or centralized); Record Locator Service; all types of Queries/Pulls; and EHI return to an authorized requesting Qualified HIN. The Qualified HIN's Broker service must return EHI from across all of the Qualified HIN's Participants and their End Users in a single transaction or, upon request of the initiating Qualified HIN, provide a list of all EHI locations back to the initiating Qualified HIN's Broker and, if further requested by the initiating Qualified HIN, subsequently return the requested EHI to the initiating Qualified HIN.	Requiring inclusion of a Connectivity Broker in the QHIN will likely reduce the number of potential QHINs and require models like RLSs that may not be needed in newer technology approaches.
		Covered Entity: has the meaning assigned to such term at 45 C.F.R. §160.103 of the HIPAA Rules.	
		Current USCDI: the version of the USCDI for which updated APIs and data formats are then required under Section 2.3 below as of the date on which the Query/Pull is initiated.	Please see The Sequoia Project's comments on the USCDI, submitted separately.
		Data: one or more elements of EHI (unless otherwise expressly specified). If the word data is not	

		capitalized, the foregoing definition shall not apply. Disclosure: has the meaning assigned in 45 C.F.R. §160.103 of the HIPAA Rules.	
25	Definitions	**Discovery**: for purposes of determining the day on which a Breach was discovered, the term discovered shall have the same meaning assigned to it in 45 C.F.R. §164.404 of the HIPAA Rules. **Directed Query**: an electronic method of requesting EHI (sometimes referred to as a pull) that asks only specific Participants and/or End Users if they have EHI on an individual or set of individuals. **Electronic Health Information (EHI)**: any health information regarding an individual that is transmitted by or maintained in electronic media, as defined in 45 C.F.R. 160.103, and includes but is not limited to Electronic Protected Health Information. EHI also includes electronic health data accessed, exchanged or used in the context of the Trusted Exchange Framework and refers to all electronic health-related data developed for an individual, on behalf of an individual or received from an individual that relates to the past, present or future health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual. EHI may, for example, be provided directly from an individual or from technology that the	

		individual has elected to use. It is not required to have been created or received by a health care provider, health plan, public health authority, employer, life insurer, school, university or health care clearinghouse. **Electronic Protected Health Information (ePHI):** has the meaning set forth in 45 C.F.R. §160.103 of the HIPAA Rules. End Entity: a user of public key infrastructure (PKI) digital certificates or an end user system that is the subject of a PKI digital certificate. **End User**: an individual or organization using the services of a Participant to send and/or receive EHI. **End User Obligations**: all of the obligations of End Users set forth in Section 10 below or elsewhere in these terms and conditions. **FALs: the Federation Assurance Levels** described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017). **Fees**: all fees and other amounts charged by a person or entity with respect to the services provided by the person or entity in connection with the Common Agreement. Fees may include but not limited to, one-time membership fees, ongoing membership fees, testing fees, ongoing usage fees, transaction fees, data analytics fees, and any other present or future obligation to pay money or provide any other thing of value.	This is an appropriate definition.

		FIPS PUB 140-2: the Federal Information Processing Standard Publication 140-2, Security Requirements for Cryptographic Modules (May 25, 2001), part of the Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). **FHIR: the Fast Healthcare Interoperability Resources** specification to the extent formally adopted by HL7.	We ask that ONC consult with HL7 on the best definition of FHIR given its intent and to be clear on the meaning of formal adoption. In general, we suggest that the definition refer to a specific FHIR specification or, ideally, replace "the Fast . . ." with "an appropriate Fast . . . HL7 as specified by the RCE in an applicable use case implementation guide."
26	Definitions	Health Care Operations: has the meaning set forth in 45 C.F.R. §164.501 of the HIPAA Rules. Healthcare Provider: has the meaning set forth at 45 C.F.R. §160.103 of the HIPAA Rules. Health Information Network (HIN): means an individual or entity that -- (a) determines, oversees, or administers policies or agreements that define business, operational, technical, or other conditions or requirements	The very broad definition of a HIN, could include industry alliances, EHR/HIT vendors, and other organizations and individuals that do not consider themselves as networks or operate as such. This broad definition could implicate a large set of organizations in information blocking provisions in Cures, which apply to "health information networks". We suggest that ONC narrow this definition in consultation with the RCE.

		for enabling or facilitating access, exchange, or use of Electronic Health Information between or among two or more unaffiliated individuals or entities; (b) provides, manages, or controls any technology or service that enables or facilitates the exchange of Electronic Health Information between or among two or more unaffiliated individuals or entities; or (c) exercises substantial influence or control with respect to the access, exchange, or use of Electronic Health Information between or among two or more unaffiliated individuals or entities. HIN Agreement: the written agreement between a Health Information Network and a Participant that uses its services. HIPAA: the Health Insurance Portability and Accountability Act of 1996 codified at 42 U.S.C. § 300gg, 29 U.S.C § 1181 *et seq.* and 42 USC 1320d *et seq.* and the Health Information Technology for Economic and Clinical Health Act (HITECH) codified at 42 U.S.C. §§ 17921 *et seq*.	

		HIPAA Rules: as set forth in 45 C.F.R. Parts 160, 162 and 164 and as amended (as applicable) as of the date in question. HL7: Health Level Seven International, a standards developing organization. IAL2: Identity Assurance Level 2 described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017). IHE: IHE International, Inc., a not for profit corporation (sometimes also referred to as Integrating the Healthcare Environment). IHE XCA: the cross-community access profile that supports the means to query and retrieve individual relevant medical data held by other communities then most recently formally adopted by IHE. Individual: Includes the following: an individual as defined by 45 C.F.R. § 160.103, as amended; any other person who is the subject of the electronic health information being accessed, exchanged, or used; a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g), as amended; a person who is a legal representative of and can make health care decisions on behalf of an individual described in this definition; or an executor, administrator or other person having authority to act on behalf of a deceased individual or the individual's estate under State or other law.	Please confirm with IHE that "formally adopted" is the right formulation.

27	Definitions	Individual Access: 1) With respect to the Permitted Purposes definition, an individual's right to access and obtain a copy of ePHI pursuant to all Applicable Law including, without limitation, 45 C.F.R. §164.524 which sets forth the right of an individual to direct that a copy of ePHI in one or more designated record sets be transmitted to another person designated by the individual. Individual includes a personal representative of the individual in question to the extent permitted under Applicable Law. 2) With respect to a Query/Pull for Individual Access, the response shall be provided as required by these terms and conditions regardless of whether it was initiated for the individual by a consumer or patient-facing application or product selected by the individual that complies with all appropriate privacy and security requirements of this agreement and Applicable Law	We note that this section gives broad "rights" to apps and similar products but also requires, positively, that they comply with this agreement and applicable law. We also ask ONC to clarify what it means for the app to be "connected to" a Participant or End User.

		and is connected to or is itself a Participant or an End User. **Information Blocking**: has the meaning set forth in 42 U.S.C. § 300jj–52 and any applicable regulations promulgated thereunder that are then in effect. **ISA**: the reference guide version of the Interoperability Standards Advisory then most recently published by ONC on its website or any successor to such document subsequently designated by ONC. **NHIN Authorization Framework 3.0 specification:** the specification formally adopted for the Nationwide Health Information Network. **NIST Special Publication 800-63:** National Institute of Standards and Technology Special Publication 80063 (Revision 3), Digital Identity Guidelines. **OASIS: the Organization for the Advancement of Structured Information Standards**, a nonprofit consortium. **OAuth 2.0**: an authorization framework developed by the Internet Engineering Task Force (IETF) OAuth Work Group. **Onboard**: all implementation and other activities necessary for a Participant to become operational in the live environment of a Qualified HIN. **ONC**: the Office of the National Coordinator for Health Information	Does the ISA have a formal publication date or is it a rolling update document? https://www.healthit.gov/isa/recent-isa-updates. The definition should probably refer to the annual "reference edition".

		Technology of the U.S. Department of Health and Human Services. OpenID Connect: an interoperable authentication protocol based on the OAuth 2.0 family of specifications promulgated by the OpenID Foundation. **Participant**: a person or an entity that participates in a Health Information Network that is a Qualified HIN. Without limitation of the foregoing, a health information exchange could be a Participant with respect to a Qualified HIN.	
28	Definitions	**Participant Agreement**: an agreement between a Participant and each of its End Users. **Participant Obligations**: all of the obligations of Participants set forth in Section 9 below or elsewhere in these terms and conditions. **Payment**: has the meaning set forth in 45 C.F.R. §164.501 of the HIPAA Rules. **Permitted Purposes**: Use or Disclosure for Treatment, Payment, Health Care Operations, Public Health, Individual Access, and Benefits Determination as permitted and pursuant to an Authorization and to the extent permitted under Applicable Law.	This definition, focusing on HIPAA permitted purposes, is inconsistent with common best practices today, under which the definition of permitted purposes focuses on the reason for which data are initially requested and transmitted, rather than subsequent use and disclosure of the data. As written, the definition would put constraints on future uses, which we recommend should defer to applicable law.

		Population Level: a type of exchange of EHI of multiple individuals in a single transaction, sometimes referred to as a bulk transfer. **Protected Health Information (PHI)**: has the meaning set forth in 45 C.F.R. §164.501 of the HIPAA Rules. **Public Health**: with respect to the definition of Permitted Purposes, a use or disclosure permitted under the HIPAA Rules and any other Applicable Law for public health activities and purposes, including, without limitation, 45 C.F.R. §164.512(b) and 45 C.F.R. §164.514(e) of the HIPAA Rules. **Qualified HIN**: a Health Information Network that meets the following criteria and has agreed to the Common Agreement including the terms and conditions set forth herein : (a) Is an entity that provides the ability to locate and transmit EHI between multiple persons and/or entities electronically, on demand or pursuant to one or more automated processes; (b) Controls and utilizes a Connectivity Broker service for all EHI exchange subject to the Common Agreement;	We recommend, per our comment letter, that the definition of a QHIN be modified to allow for greater diversity of participation.

		(c) Is Participant neutral, meaning that none of the exchanges of EHI by or on behalf of the Qualified HIN include the Qualified HIN itself (whether directly or indirectly) as one of the parties except to the extent that the Qualified HIN receives and maintains such EHI as part of a repository it maintains as a Health Information Network but does not Use or Disclose it except to the extent permitted as a Business Associate under the HIPAA Regulations and other Applicable Law; (d) Has Participants that are actively exchanging EHI in the data classes included in the then Current USCDI in a live clinical environment in accordance with Section 3 and Section 6 below; and (e) Demonstrates that it has mechanisms in place, whether by contract or otherwise, (1) to impose all of the Participant Obligations on all Participants who provide or have access to any of the Health Information Network's services; and (2) whether directly or indirectly,	We believe that the definition of participant neutrality will unnecessarily limit the number of organizations that can qualify as a QHIN. We believe that this definition would preclude newer or specialized HINs from being a QHIN. We believe that ONC should permit specialized (e.g. by use case and technology) QHINs and ensure as well that Participants that have specialized missions can participate as well. Participants will work with QHINs that best meet their needs.

		to audit Participants' compliance with all relevant obligations and provide for appropriate remedial action (up to and including exclusion) against any Participant that fails to comply with the same. **Query/Pull**: includes both Directed Query and any type of Broadcast Query.	
29	Definitions	**Reasonable Allowable Cost**: costs of a Qualified HIN that: (a) were actually incurred; (b) were reasonably incurred; (c) are either the direct costs of providing the Attributable Services or are a reasonable allocation of indirect costs of providing the Attributable Services; and (d) are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. **Recognized Coordinating Entity (RCE)**: the entity selected by ONC that will enter into agreements with HINs that qualify and elect to become Qualified HINs in order to impose, at a minimum, the requirements of	We agree with the principle of promoting reasonably priced services; however, we question the prescriptive nature of the proposed methodology. We believe that further clarification is needed in defining "reasonable" costs, and also suggest that margin should be considered an allowable cost. This approach would likely require significant cost accounting, increasing ecosystem costs and potentially discouraging QHIN participations. We do note and ask ONC to clarify that the concept of Reasonable Allowable Costs only applies to QHINs with respect to charges to other QHINs. Overall, we suggest that ONC focus on fee transparency rather than introducing detailed requirements. As discussed in our formal comment letter, we support ONC's intention to use a private sector organization as the RCE.

		the Common Agreement on the Qualified HINs and administer such requirements on an ongoing basis as described herein. Record Locator Service (RLS): a service that provides the ability to identify where records are located based upon criteria such as an individual's demographic data and/or record data type, as well as providing functionality for the ongoing maintenance of this location information. **SAML (Security Assertion Markup Language**): an open standard for exchanging authentication and authorization data between parties, in particular, between an identify provider and a service provider, which has been adopted by OASIS. **SHA-2 (Secure Hash Algorithm 2):** a set of cryptographic hash functions designed by the U.S. National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). **SOAP (Simple Object Access Protocol**): a protocol specification for exchanging structured information in the implementation of web services in computer networks introduced by several vendors. **SSL (Secure Sockets Layer**): a security protocol for establishing encrypted links between a web server and a browser in an	

		online communication, a standard adopted by the Internet Engineering Task Force (IETF). **Standard Agreement**: the written agreement between the RCE and a Health Information Network that uses its services. **TEFCA: the Trusted Exchange Framework and Common Agreement** then in effect and published in the Federal Register and on ONC's website. **TPO**: Treatment, Payment and Health Care Operations. **TLS (Transport Layer Security**): a cryptographic protocol that provides communication security over a computer network, a standard adopted by the Internet Engineering Task Force (IETF). **Treatment**: has the meaning set forth at 45 C.F.R. §164.501 of the HIPAA Rules. Use: has the meaning assigned in 45 C.F.R. §160.103 of the HIPAA Rules.	
30`	Definitions	**US Core Data for Interoperability (USCDI):** As adopted and updated from time to time by HHS, a minimum set of data classes (including, without limitation, specified clinical data fields) that should be exchanged when the data is available. Whitelist: a list of e-mail addresses or IP addresses from which an application blocking program will allow messages to be received.	Please see The Sequoia Project's comments on the USCDI, submitted separately

		XSPA Profile (Cross-Enterprise Security and Privacy Authorization Profile): a profile which has been adopted by OASIS. **XUA Profile (Cross-Enterprise User Assertion Profile)**: a profile that is part of the IHE International IT Infrastructure Technical Framework. **X.509**: a standard for digital certificates promulgated by the International Telecommunication Union (ITU) that uses the international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.	
30	2. Requirements of Qualified HINs		We note that the requirements in this section are quite significant and will likely require substantial changes to Participation Agreements, and suggest that more than 12 months may be needed to obtain participant community buy-in, including formal federal agency review, for updated terms.
30	Requirements	2.1 No Limitations on EHI Aggregation. A Qualified HIN shall not limit the aggregation of EHI that is exchanged among Participants, provided that any such EHI aggregation is in support of the Permitted Purposes and in accordance with all Applicable Law.	
30	Requirements	2.2 Permitted and Future Uses of EHI. Once EHI is shared with another Qualified HIN, the receiving Qualified HIN may	2.2 – We suggest that ONC clarify that this provision applies only to QHINs in their role of transmitting data in response to queries and not to HINs and their participants. We note that the definition of Participant Agreement is “an

		exchange, retain, Use and Disclose such EHI only to perform functions in connection with the Permitted Purposes in accordance with the Common Agreement and the Qualified HIN's Participant Agreements or as otherwise permitted by Applicable Law.	agreement between a Participant and each of its End Users"; and thus, is not the agreement between a QHIN and its own Participants as noted in 2.2. It will be very important for ONC to use this term consistently in the TEFCA.
30	Requirements	2.3 Mandatory Updating of the USCDI. Each Qualified HIN shall update its data format and/or API to include new data classes (including, without limitation, specified clinical data fields) added to the USCDI within a reasonable time (not less than twelve (12) months) after the date of the data classes being officially added to the USCDI.	2.3 - This requirement assumes that the Qualified HIN controls the format of data being exchanged by its Participants. The QHIN may be a pass-through only, which means that they could only accomplish updates to data formats indirectly, through contract.
	Requirements	2.4. Implementation of API. Each Qualified HIN shall implement the APIs necessary to perform its obligations hereunder within twelve (12) months of the date of the API Implementation Guide being formally adopted by HL7 on its public website and recognized by ONC on its public website. For any additional standards necessary for the Qualified HIN's Broker to facilitate interoperable transactions among Qualified HINs, the Qualified HIN shall consult and seek to have its Broker use standards identified in the then most recent ISA.	2.4 - This section refers to "the API Implementation Guide being formally adopted by HL7…". We note that "API" is defined, but "Implementation Guide" is not. Consideration should be given to how the "API Implementation Guide" is kept updated and who is responsible. We also do not believe that the FHIR specification is the API itself but rather the standard and implementation specification for APIs that will be developed by various end users and that can interoperate based on adherence to the applicable specification. We suggest that in this document, ONC be consistent in referring either to "specification" or "implementation guide" and focus on the specification designed to align with the USCDI. In addition, as indicated above, we do not think that the reference to the ISA is sufficient given its construction and intended use and urge ONC to reply on the RCE to define how the standards in the ISA, which vary in maturity and applicable use case, should be implemented in this new model. Finally, in our experience, the work products developed by SDOs and even standards acceleration initiatives like the Argonaut project, still require further refinements, testing and piloting in practice before being ready for widespread

			adoption. Therefore, we recommend that the RCE work collaboratively with ONC, QHINs, the implementation community and the standards body/ies to develop a timeline for implementation. Consideration also needs to be given to versioning and migration planning over time.
30	Requirements	2.5 Mandatory Updating of Participant Agreements. Each Qualified HIN shall update its Participant Agreements to incorporate the applicable minimum terms and conditions set forth herein within twelve (12) months of the date of the final Common Agreement being published	We suggest that the timing for required updates be revised to allow up to 18 months (and even as long as 24 months), reflecting needed time to do the analysis, update the agreements and, in the case of QHINs and HINs that involve governmental agencies, federal clearance and approval processes. ONC and CMS have recognized similar timing needs of greater than one year in certification and meaningful use/MIPS deadlines. We also suggest that the RCE establish a process to coordinate among QHINs. In addition, as indicated above, Participant Agreement seems to be defined as between the Participant and its End Users and not the QHIN and is Participants. Is ONC requiring QHINs to also define the agreements between its Participants and their End Users?
31	Requirements	2.6 Completion of Onboarding Requirements. Each Qualified HIN shall ensure that each Participant has completed the necessary requirements to Onboard to the Qualified HIN within a reasonable time and is subsequently exchanging EHI in a live environment.	2.6 - We agree with this requirement in general.
31	Requirements	2.7 Compliance with Updated Standards. Except as otherwise expressly provided herein, whenever this Agreement references any standard, implementation specification, or certification criteria to which a Qualified HIN or Participant must comply, the Qualified HIN or Participant shall not be required to comply with any updates to such standards, implementation specifications or certification criteria until twelve (12) months after such standard has	We suggest that the timing for required updates be revised to allow up to 18 months (or longer depending upon the maturity and implementation readiness of the standards), reflecting needed time to do the analysis, update the agreements and, in the case of QHINs and HINs that involve governmental agencies, federal clearance and approval processes. We also suggest that the RCE establish a process to coordinate among QHINs regarding implementation timelines for specific standards and that an RCE requirement to make changes in a shorter period than 12 or 18 months be permitted if needed for exchange to proceed effectively. We also note that other parts of the TEFCA indicate that the RCE can have additional terms/requirements, which could include other voluntarily adopted standards. We suggest working with the RCE to advise on versioning and adoption timeframes.

		been formally adopted by HHS or other applicable authority.	
31	3. Standardization		Overall, this section requires significant standardized requirements for QHINs in terms of such issues as EHI sent, patient matching data, reliance on ONC 2015 certification and associated standards. We believe that the implementation process regarding standards as coordinated through the QHIN should have greater flexibility than is reflected in the Draft TEF on standards for data exchange, including the standards to support population-level exchange. In general, we agree with the standards called for but as indicated through our comments, we believe that such specificity should be move to the RCE implementation guides, which are likely to need even greater specificity with respect to standard and implementation guide versions.
31	Standardization	3.1 Connectivity Broker (Broker) Capabilities: Each Qualified HIN shall provide the following capabilities and take the following actions using its Broker when it: (a) initiates any authorized Query/Pull to another Qualified HIN, or (b) receives an authorized request for EHI from another Qualified HIN (or anyone authorized to act on behalf of a Qualified HIN):	We suggest that ONC clarify that a QHIN can contract with a Connectivity Broker service and that Broker services could come from more than one entity, with such an entity potentially serving multiple QHINs. More generally, we suggest that such functional requirements may need to be refined over time. As a result, we recommend that functional and technical requirements be captured in an implementation guide in lieu of legal terms in an agreement. This approach will help streamline and simplify the update process.
31	Standardization	3.1.1 The Broker shall send and receive all of the EHI in the data classes included in the then Current USCDI when and to the extent such EHI is requested and electronically available within or through the Qualified HIN's Health Information Network. 3.1.2 As more fully described in the following provisions of this Section 3, the Qualified HIN's	3.1.2 - The patient matching data in the 2015 edition appear reasonable, and generally align with the approach used by The Sequoia Project initiatives. At the

		Broker shall send and receive all of the “patient matching data” so labelled and specified in the 2015 Edition certification criterion set forth at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable standards adopted in the future by HHS) when and to the extent that such data is electronically available within or through the Qualified HIN’s network to the extent permitted under Applicable Law. 3.1.3 As more fully described in the following provisions of this Section 3, the Qualified HIN’s Broker shall adhere to standards and implementation specifications for electronic data and interoperability that are outlined in 45 C.F.R. Part 170, Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation specifications adopted in the future by HHS) for the uses to which those standards and implementation specifications are applied. For any additional standards and implementation specifications necessary for the Qualified HIN’s Broker to facilitate interoperable transactions among Qualified HINs, the Qualified HIN shall consult and seek to have its Broker use standards and implementation specifications identified in the then most recent ISA 3.1.4 When a Participant initiates any Query/Pull, (a) the Participant’s Qualified HIN shall cause its Broker to initiate the Query/Pull	same time, we suggest that ONC point to more contemporary work, such as The Sequoia Project Patient Matching whitepaper, and that it enable the RCE process to adjust such requirements through an implementation guide process. 3.1.3 – The references to standards in the CFR and the 2015 edition are quite broad and we recommend that the requirements be made more specific. As we indicate elsewhere, we believe that standards specificity should not be in the TEF or the Common Agreement, but in use case -specific implementation guides. In addition, the exchange community may not agree to comply with unspecified standards and specifications adopted by HHS in the future. 3.1.4. As indicated elsewhere in our comments, we do not think that the default query should be a broadcast query as defined in the Draft TEF. It is one of several query approaches that are viable for different needs and workflows

		for all EHI in the data classes included in the then Current USCDI to the extent requested and permitted under Applicable Law, and (b) each Qualified HIN shall cause its Broker to respond to all Queries/Pulls for data classes included in the then Current USCDI to the extent requested and permitted under Applicable Law	
32	Standardization	3.1.5 Within twelve (12) months after the FHIR standard with respect to Population Level Query/Pulls has been formally approved by HL7, each Qualified HIN shall cause its Broker to be able to initiate and respond to all Query/Pulls for as many individuals as may be requested by another Qualified HIN in a single Query/Pull. 3.1.6 Each Qualified HIN shall cause its Broker to promptly and accurately enter all queries/pulls it initiates or responds to into an audit log and to maintain the audit log as required by Applicable Law. 3.1.7 The Qualified HIN shall cause the Broker to be able to initiate Queries/Pulls and respond to all Queries/Pulls with Brokers of all other Qualified HINs in accordance with both the IHE XCA standards then most recently formally adopted and the certification criterion specified at 45 C.F.R. 170 Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation	3.1.5 – See comments above re: timing. In addition, we believe that a reference should be to an implementation guide or specification and not a standard. See also comments on 8.1. 3.1.7 As with other referenced standards, our experience suggests that the RCE will need to develop additional implementation guidance to ensure effective use of the referenced standards for their intended purpose.

		specifications adopted in the future by HHS). 3.1.8 Initiating Queries. The Qualified HIN shall cause its Broker to perform the following functions when initiating any Query/Pull: **(a)** The initiating Broker of the Qualified HIN shall receive the Query/Pull request from the Qualified HIN's Participants in any format that has been agreed upon within the Qualified HIN's Health Information Network; **(b)** The initiating Broker of a Qualified HIN shall send all Queries/Pulls to the Broker of each other Qualified HIN that is then processing Queries/Pulls in a live environment pursuant to the Common Agreement using IHE XCPD or standards specified in the then applicable certification criterion at 45 C.F.R. 170 Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation specifications adopted in the future by HHS); **(c)** Upon receiving confirmation from the responding Broker that an individual's EHI is available, the initiating Broker of the Qualified HIN shall send a Query/Pull to the Broker of each other Qualified HIN that confirmed EHI availability, using IHE	3.1.8 and 3.1.9: We wish to note that these requirements, which are described in a little more than one page, are addressed by pages 34-79 of Carequality's Query-Based Document Exchange Implementation Guide. We do not disagree with keeping the TEFCA at a higher level, but want to emphasize importance of using RCE implementation guides to contain operational requirements. 3.1.8 (b) – We question whether it is practicable to contractually require that a QHIN query every other existing QHIN, every time it launches a query for any purpose. Based on our experience, there are many cases in which it would be reasonable to query a single QHIN, (e.g. a notification has been received of an event at a specific organization served by a known QHIN).

		XCA or standards specified in the certification criterion at 45 C.F.R. 170 Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation specifications adopted in the future by HHS) that would complement or replace a format described herein; **(d)** When performing each Query/Pull, the Qualified HIN's Broker shall identify the specific Permitted Purpose for the Query/Pull using a SAML token for the message in accordance with the NHIN Authorization Framework 3.0 specification, Section 3.2.2.6, Purpose of Use Attribute or any successor specification subsequently formally adopted or specified by HHS; **(e)** The initiating Qualified HIN shall cause its Broker to consolidate results from all Brokers of other Qualified HINs that respond; and **(f)** When delivering responses to an initiating Qualified HIN's own Participant that were received from another Qualified HIN in response to Queries/Pulls from the initiating Qualified HIN's own Participant, the Broker of the initiating Qualified HIN may use any internally defined interactions (such as individual matching, provider identity, or data transmission) to send EHI to the	

		initiating Qualified HIN's own Participant.	
33	Standardization	3.1.9 Responding to Queries/Pulls. The Qualified HIN shall cause its Broker to perform the following functions when responding to any Query/Pull from any other Qualified HIN. **(a)** The responding Qualified HIN's Broker shall use a Brokered Broadcast Query to determine the Participant and Qualified HIN systems which hold the EHI requested, subject to any limitations set forth in the Query/Pull and to the extent permitted by Applicable Law; **(b)** The responding Qualified HIN's Broker may use any internally defined interactions (such as individual matching, provider identity, data transmission) to retrieve all of the EHI in the data classes included in the then Current USCDI from its Participants as long as it responds to the initiating Qualified HIN's Broker in accordance with the other requirements of this Section 3. Additionally, regardless of the format and any problems that may arise from the format in which the Participant entered the EHI or makes it available for a response, the responding Broker is responsible for	(b) - We strongly agree that QHINs should have flexibility in how they architect internal interactions. At the same time, we do not believe that the TEFCA should specify how a responding broker handles the results from multiple participants.

		returning all of the EHI in the data classes included in the then Current USCDI, when and to the extent that such EHI is available and has been requested and the response is in compliance with Applicable Law; and **(c)** If more than one Participant internal to the Qualified HIN's Health Information Network has the desired EHI, the responding Broker shall consolidate the results from the multiple Participants into one response to the initiating Broker.	
33	Standardization	3.2 USCDI 3.2.1 Each Qualified HIN shall exchange all of the EHI in the data classes in the then Current USCDI to the extent such EHI is then available from its Participants and has been requested and to the extent permitted by Applicable Law. 3.2.2 All Participants of a Qualified HIN that collect and maintain EHI in the data classes included in the then Current USCDI, upon request, shall provide all such EHI to fulfill such request to the extent the EHI is available and	3.2 - As the USCDI expands, and even with its proposed addition of clinical notes, we question whether the establishment of multiple levels of obligations to maintain data in standardized form and make it available, will be a source of concern and confusion. We therefore urge ONC to consider this issue and to work with the RCE to address these concerns to ensure maximum participation in and usability in the exchange process. It is unclear what the relationship is between this proposal, and the current C-CDA based exchange models. We suggest that ONC clarify whether the C-CDA templates and FHIR resources in general use today can accommodate new USCDI data categories

		permitted under Applicable Law.	
33	Standardization	3.3 Patient Demographic Data for Matching 3.3.1 Each Qualified HIN shall support the exchange of the patient matching data enumerated in the 2015 Edition certification criterion adopted at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable certification criteria adopted in the future by HHS) to the extent permitted by Applicable Law. 3.3.2 Participants who collect and maintain the patient matching data enumerated in the 2015 Edition Certification Criterion adopted at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable certification criteria adopted in the future by HHS) shall provide all such data to the extent permitted by Applicable Law when initiating or responding to Queries/Pulls	3.3.1. See our prior comments on patient matching data elements. 3.3.2 – We agree with this criterion.
34	Standardization	3.4 Data Quality Characteristics 3.4.1 To ensure that Qualified HINs exchange accurate patient demographic data that is used for matching, Qualified HINs shall annually evaluate their patient demographic data management practices using the then current ONC Patient Demographic Data Quality Framework. The first such evaluation shall be conducted within twelve (12) months after the first version of the ONC Patient Demographic	3.4.1 – We agree with this approach of a 12-month review cycle.

		Data Quality Framework has been published in final form on ONC's website.	
34	4. Transparency		
34	Transparency	4.1 Agreements and Fee Schedules 4.1.1 Access to Agreements. Qualified HINs shall make available, respectively, their Standard Agreements and Participant Agreements to ONC and the RCE upon request. 4.1.2 Publication of Fee Schedule. Within fifteen (15) days after signing the Common Agreement, each Qualified HIN shall file with ONC a schedule of Fees used by the Qualified HIN relating to the use of the Qualified HIN's services provided pursuant to the Common Agreement that are charged to other Qualified HINs and/or Participants. If any of the Fees change while the Common Agreement is in effect, the Qualified HIN changing such Fees shall file an updated disclosure of the Fees with ONC within thirty (30) days after the effective date of such change. For purposes of this filing requirement, a change in Fees shall include any change in Fees, waiver of Fees or additional Fees that the Qualified HIN applies to all Qualified HINs and/or Participants or to any one or more of the Qualified HINs or Participants. When filing such fee schedule with ONC, the Qualified HIN shall clearly label all information with respect to Fees that may	4.1.1 – We agree with the requirement to make agreements available as indicated. 4.1.2 - We believe that this requirement could substantially limit flexibility on fee negotiations based on specific circumstances and on periodic updates, especially with respect to fees charged by the QHIN to its participants. This latter restriction may hinder the willingness and ability of organizations to participate as QHINs.

		contain trade secrets or commercial or financial information that is privileged or confidential.	
		4.2 Publication of USCDI Data Classes. Each Qualified HIN shall publish and maintain on its public website a list of each of the data classes from the then Current USCDI that the Qualified HIN supports for any and all of the Permitted Purposes.	4.2 – We suggest that ONC define “support” for a data class and also identify the extent to which QHINs have choices in which Data Classes to support. In addition, given 3.1.9, we ask ONC to indicate whether the supported data classes can vary by permitted purpose, which we encourage.
		4.3 Disclosures for Patient Safety, Public Health and Quality Improvement Purposes. Upon request, each Qualified HIN shall disclose information to the Participants and other entities described below for the following patient safety, public health, and quality improvement purposes to the extent permitted by Applicable Law: (i) sharing comparative user experiences that may affect patient care; (ii) developing best practices for health information exchange and clinician use; (iii) reporting of EHR-related adverse events, hazards, and other unsafe conditions to government agencies, accrediting bodies, patient safety organizations, or other public or private entities that are specifically engaged in patient quality or safety initiatives; (iv) conducting research studies for peer-reviewed journals; (v) participating in cyber threat sharing activities; and (vi) identifying security flaws in the operation of the Qualified HIN that would not otherwise fall into subsection (v).	4.3 Overall, we question the extent to which QHINs would or should have access to the information in (i), (ii), and (iii).

		Participants that are Covered Entities or Business Associates should consider their HIPAA Privacy and Security Rule obligations before sharing EHI for these purposes.	
35	5. Cooperation and Non-Discrimination		As indicated below, we have questions and issues with elements of this section, based on our experience.
35	Cooperation and Non-Discrimination	5.1 Permitted Purposes and EHI Reciprocity. To the extent permitted by Applicable Law, each Qualified HIN shall support all of the Permitted Purposes by providing, upon request, all of the EHI in the then current USCDI to the extent the EHI is available.	5.1 We read this provision's primary intent as ensuring that each QHIN, in its role as a query responder, will honor queries for all permitted purposes and from any other QHIN. If this is correct, we suggest that the wording be clarified to indicate that the terms' context is a QHIN's role as a query responder. We also suggest that the word "reciprocity" not be used, since in many circumstances different QHINs will likely serve different customer types and make requests for different permitted purposes. A QHIN that primarily serves payers, for example, may have little reason in actual practice to query a QHIN that primarily serves insurers participating in the Benefits Determination permitted purpose.
35	Non-Discrimination	5.2 Non-Discrimination. 5.2.1 A Qualified HIN may not require exclusivity or otherwise prohibit (or attempt to prohibit) any of its Participants from joining, exchanging EHI with, conducting other transactions with, using the services of, or supporting any other Qualified HIN.	5.2.1 This is appropriate.

		5.2.2 A Qualified HIN shall not unfairly or unreasonably limit exchange or interoperability with any other Qualified HIN, such as by means of burdensome testing requirements that are applied in a discriminatory manner, sending EHI at different speeds (sometimes referred to as data throttling), or other means that limits the ability of a Qualified HIN to send or receive EHI with another Qualified HIN or slows down the rate at which such EHI is sent or received. As used in this Section 5, a discriminatory manner means action that is taken or not taken with respect to any Qualified HIN, Participant or End User, or group of them due to the role it plays in the healthcare system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that different treatment shall not be deemed discriminatory to the extent that it is based on a reasonable and good faith belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the Common Agreement (including compliance with Applicable Law) in any material respect. For example, imposing different testing requirements on a Qualified HIN because it primarily serves providers that are not users of a certain electronic health record system or because it primarily serves	5.2.2 This provision is reasonable so long as the focus is on a clear definition of discriminatory. In general, we think that testing and onboarding requirements should be uniform across all QHINs within the TEFCA model. We do want to note, however, that not all testing is burdensome. There are legitimate and very important reasons that testing is necessary. For instance, in our experience, testing is necessary to assure that other QHINs and their participants have securely configured their production systems, as well as X.509 digital certificates. Additional testing is often necessary to verify the clinical content being exchanged complies with the standards and implementation guides, and to have greater assurance of data quality and completeness and reproducibility of content that is of value to end users. We wish to call out that several federal agencies, for instance, have specific expectations in terms of data content requirements in support of their programs. We encourage ONC to distinguish discriminatory practices from very practical, real-world operational needs. Over time, we have observed that rigorous testing raises the bar and helps mature implementations, which often results in reduced testing requirements over time.

		payers would be considered discriminatory for purposes of this Section. 5.2.3 In revising and updating its Broker from time to time, a Qualified HIN will use commercially reasonable efforts to do so in accordance with generally accepted industry practices implemented in a manner that will not cause other Qualified HINs unreasonable cost, expense or delay in executing Queries/Pulls from the revised or updated Broker; provided, however, this provision shall not apply to the extent that such revisions or updates are required by Applicable Law or in order to respond promptly to newly discovered privacy or security threats. 5.2.4 Each Qualified HIN shall use commercially reasonable efforts to provide reasonable prior written notice of all revisions or updates of its Broker to all other Qualified HINs and to the Recognized Coordinating Entity if such revisions or updates could adversely impact the exchange of EHI between Qualified HINs or require changes in the Brokers of any other Qualified HIN regardless of whether they are necessary due to Applicable Law or newly discovered privacy or security threats.	5.2.3 This is reasonable but the RCE and QHIN community will need flexibility to agree upon and implement specific best practice guidelines as experience dictates. 5.2.4 This appears reasonable

35-36	Cooperation and Non-Discrimination	5.3 Fees.	
		5.3.1 A Qualified HIN must use reasonable and non-discriminatory criteria and methods in creating and applying pricing models if it charges any fees, or imposes any other costs or expenses on another Qualified HIN. Nothing in these terms and conditions requires any Qualified HIN to charge or pay any amounts to another Qualified HIN. Subject to the further limitations set forth below, only the Qualified HIN's Attributable Costs may be charged to another Qualified HIN.	5.3.1- We agree with the importance of having reasonable and non-discriminatory criteria and methods related to charging fees to other QHINs. Based on our experience with Sequoia Project initiatives, clarity on permissible fees and when and how they can be applied is essential. Specifically, we question the practicality of a fee structure if there is not an obligation to pay. Further, we question how an obligation to pay will be established, if QHINs are forbidden to have additional agreements with one another beyond the TEFCA.
		5.3.2 A responding Qualified HIN may charge an initiating Qualified HIN an amount equal to the responding Qualified HIN's Attributable Costs for responding to Queries/Pulls by the initiating Qualified HIN only if they were incurred for the Permitted Purposes of Treatment, Payment, or Health Care Operations. Notwithstanding anything to the contrary set forth in the Common Agreement or elsewhere, a responding Qualified HIN may not charge any amount for responding to Queries/Pulls for the Permitted Purposes of Individual Access, Public Health or Benefits Determination.	5.3.2 - We are unclear on the rationale for permitting fees for TPO but not for the other permitted purposes. Certainly, these other uses cases could also involve costs for the QHINs warranting fees under the same rationale that fees for TPO are permitted. In addition, we are unclear why only costs associated with Attributable Costs as defined earlier (see our comments on that definition) are permitted, especially with respect to costs for services that are already being provided by a QHIN.
		5.3.3 A Qualified HIN may not impose any royalty, revenue sharing, or other fee on the	5.3.3 We ask ONC to clarify if this provision means that a QHIN can't themselves benefit from secondary use after the EHI has been accessed or that they can't charge a royalty or other to another QHIN based on its access and subsequent secondary use.

		use of the EHI (including secondary uses) once it is accessed by another Qualified HIN.	
36		5.4 Broadcast and Directed Queries. Except as required by the HIPAA Rules or other Applicable Law, no Qualified HIN shall enter into any agreement other than the Common Agreement with another Qualified HIN who has also adopted the Common Agreement with respect to any Broadcast Query or Directed Query with respect to any of the Permitted Purposes.	5.4 We are unclear why other agreements between QHINs are prohibited, even if they are not in conflict with the CA. We believe this may have unintended consequences. For instance, additional agreements would be necessary in order for QHINs to address financial arrangements should QHINs charge each other fees, as noted above.
36	6. Privacy, Security, and Patient Safety		
36	6.1 Privacy Requirements		
36-38		6.1.1 Individual Access. Each Qualified HIN agrees and acknowledges that individuals have a right to access, share and receive their available ePHI in accordance with the HIPAA Rules, section 4006(b) of the 21st Century Cures Act, and the terms and conditions of the Common Agreement. Each Qualified HIN agrees and acknowledges that individuals have a right to direct a HIPAA Covered Entity to transmit a copy of ePHI in a designated record set to any third parties designated by the individual in accordance with Applicable Law. Similarly, each Qualified HIN agrees and acknowledges that individuals have a right to	6.1.1 With respect to an individual's right to direct a Participant or End User that is NOT a Covered Entity to transmit a copy of EHI to a third party: - We ask ONC to clarify if this is a right under HIPAA (even if this obligation is not addressed in a HIPAA Business Associate Agreement) or a right that is established under the TEFCA. Fundamentally, we ask ONC to clarify the obligation of a Participant or End User under HIPAA vs. the underlying Covered Entity/provider who holds/originates the data. In addition, we believe that clarity is needed in distinguishing between an individual's request for records, which the individual can then direct as he or she pleases, and an individual's request that a Covered Entity transmit a copy of his or her EHI to a third party. The former is directly supported by the standards and operational approaches outlined in the TEF, but the latter, while a right under HIPAA, is not actually supported by the draft TEF's outlined standards and approaches and would need to be accomplished by other means.

		direct a Participant or End User to transmit a copy of EHI to any third parties designated by the individual in accordance with Applicable Law.	
		6.1.2 Permitted and Future Uses and Disclosures of ePHI. Once ePHI is shared with another Qualified HIN, the receiving Qualified HIN may exchange, retain, Use and Disclose such ePHI only to perform functions in connection with the Permitted Purposes in accordance with the Common Agreement and the Qualified HIN's Participant Agreements, or as otherwise permitted by Applicable Law.	6.1.2 – In our experience, Permitted Purposes typically apply to the purpose for which data is being requested or transmitted, with future uses governed by applicable law. The proposed requirement appears consistent with what HIPAA, for instance, would expect of Covered Entities and Business Associations. To that end, the limitation on permitted and future uses for QHINs may be appropriate provision. We suggest that this be subject to further consideration by ONC and the RCE to identify and provide any needed flexibility for particular circumstances. For example, a record locator service might want to note to that an organization querying for a patient, is a likely record location for that patient.
		6.1.3 Breach Notification. When acting as a Business Associate, the Qualified HIN shall comply with all applicable Breach notification requirements regarding ePHI pursuant to 45 CFR §164.410 of the HIPAA Rules. Following discovery of a Breach of ePHI or EHI, the Qualified HIN further shall notify, in writing, the RCE without unreasonable delay, but no later than fifteen (15) calendar days, after Discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations. Upon receipt of such notice, the RCE shall be responsible for notifying, in writing, other Qualified HINs affected by the Breach within seven (7) calendar days.	6.1.3 – We ask that this provision clarify that the QHIN community and the RCE would have discretion to develop a process for QHINs to notify each other and the RCE, rather than inserting the RCE into the notification process directly.
		6.1.4 Demand for Compulsory Disclosures. If the Qualified HIN is requested or required	

		(by oral questions, interrogatories, requests for information or documents, subpoena, civil investigation, demand or similar process) to disclose any ePHI in connection with a Breach of ePHI, then the Qualified HIN shall provide to the Participant prompt written notice of such request(s), unless such notice is not permitted by Applicable Law, so that the Participant may seek an appropriate protective order and/or waiver of compliance with the provisions of the Common Agreement. In the event that such protective order or other appropriate remedy to prevent such disclosure is not obtained, the Qualified HIN may disclose only that portion of the ePHI (and only to those persons or entities) which is legally required, and the Qualified HIN agrees to reasonably cooperate to the extent permitted by Applicable Law in securing assurances that the disclosed ePHI will be accorded confidential treatment. 6.1.5 Law Enforcement Exception to Breach Notification. If a Qualified HIN is notified, in writing, by any law enforcement official, that a Breach notification would impede a criminal investigation or cause damage to national security, then the Qualified HIN shall delay the Breach notification for the time period specified by the law enforcement official in accordance with the requirements of 45 C.F.R. §164.412 and 45 C.F.R. §164.528(a)(2).	

		6.1.6 Consent. If and to the extent that Applicable Law requires that an individual's consent to the Use or Disclosure of his or her EHI, the Participant of a Qualified HIN (or the End User of such a Participant) that has a direct relationship with the individual shall be responsible for obtaining and maintaining the consent of the individual (each a "Qualified HIN's Consenting Individual") consistent with the applicable requirements. Each Qualified HIN shall specify such responsibility in its Participant Agreements. Each Qualified HIN shall require its Participants to provide the Qualified HIN with a copy of each consent of a Qualified HIN's consenting individual and the Qualified HIN shall maintain copies of such consents and make them available electronically to any other Qualified HIN upon request. 6.1.7 Revocation of Consent. Consistent with Applicable Law, each Qualified HIN agrees to maintain policies and procedures to allow an individual to withdraw or revoke his or her permission for the Use and Disclosure of the individual's EHI as obtained under Section 6.1.6 on a prospective basis. 6.1.8 Written Notice. Each Qualified HIN agrees to publish and make publicly available a written notice in plain language that describes each Qualified HIN's privacy practices regarding the access, exchange, Use and	6.1.6 –This is a very complex provision, and we question if it is actually necessary for the QHIN to specify responsibility for obtaining consent when this responsibility is largely inherent in Applicable Law. We suggest that the final TEFCA accommodate a variety of consent structures that align with HIPAA and the intent of this provision, such as the approach supported in Carequality's recent Query-Based Document Exchange Implementation Guide updates, which permit a consent to be collected remotely, by the party requesting that information be released. We also question why a QHIN must maintain copies of all consents and make them available electronically to any other QHIN upon request. In cases of consents collected by the party that is releasing the individual's record – which will likely be a common scenario – we do not believe that other QHINs will need to access the consents.

		Disclosure of ePHI with substantially the same content as described in 45 CFR §164.520(b). The written notice must contain a description, including at least one (1) example of each type of Permitted Purpose. If a Qualified HIN is a Covered Entity, the Qualified HIN's Notice of Privacy Practices must meet the requirements of 45 CFR §164.520	
38	6.2 Minimum Security Requirements	6.2. Minimum Security Requirements. To ensure the confidentiality, integrity, and availability of ePHI and consistent with the Security Rule, each Qualified HIN (a Business Associate under the HIPAA Rules) shall be required to implement the following minimum security requirements described below within twelve (12) months from the date the TEFCA is published in the Federal Register, unless otherwise specified below. As a Business Associate, each Qualified HIN acknowledges that it is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making Uses and Disclosures of ePHI that are not authorized by its contract or required by Applicable Law. Each Qualified HIN further acknowledges that a Business Associate is directly liable and subject to civil penalties for failing to safeguard ePHI in accordance with the HIPAA Security Rule.	6.2 – In general, we believe that this section is a good example of why it is important to separate many implementation details from the underlying Common Agreement (CA) legal contract. Such an approach allows the legal agreement to be stable, as technical security details will be updated more frequently than is feasible or desirable for the CA. Section 6.2.3 is also a good example of this issue, because it attempts to merge into one contract the requirements for two separate exchange paradigms (SOAP and FHIR). We highlight a few other key questions raised by Section 6.2 and its components: • What are the responsibilities of the RCE in monitoring the requirements of QHINs that are laid out in each of the 6.2 subsections? • This section's requirements are often very specific, but at times lack a unifying thread or clear articulation of a big-picture approach. • As standards evolve, what are the specific responsibilities of the RCE with respect to updating these requirements? • There are requirements that allude to certificate authorities, but more clarity is needed on the overall certificate approach that is envisioned. The current draft has many details that are not defined, for example, from 6.2.9 (iv), what is an "approved trust chain, which is not a defined term? • We seek clarification of the role of the RCE, if any, with respect to certificate management.

			• Overall, we recommend that the RCE and the implementation community be given flexibility to agree upon a certificate approach, and to address the details of the approach in use case-specific implementation guides.
38	Security	6.2.1 HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework (CSF). In addition to complying with the HIPAA Security Rule and the 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications, each Qualified HIN shall evaluate its security program on at least an annual basis. As part of its ongoing security risk analysis and risk management program, this evaluation must include a review of the NIST CSF HIPAA Security Rule Mapping, the ONC/OCR HIPAA Security Risk Assessment Tool, and the ONC Guide to Privacy and Security of Electronic Health Information, as tools to help ensure its compliance with the HIPAA Rules and to improve its ability to secure ePHI and other critical information and business processes. To the extent that a review of the NIST CSF HIPAA Security Rule Mapping identifies any gaps in the Qualified HIN's compliance with the HIPAA Rules or other Applicable Law, then the Qualified HIN shall assess and implement evolving technologies and best practices that it	6.2.1 We are not certain that the ONC 2015 security criteria are generally applicable to QHINs since the certification criteria were not written for HINs. Further, we suggest that contractually enforcing reliance on specific artifacts published by ONC and NIST may be problematic given the rapid evolution of security threats and best practices. We recommend that QHINs be given flexibility to rely on then-current cybersecurity best practices, without reference to specific artifacts. This approach admittedly sacrifices some specificity in order to maintain flexibility, but we believe it provides a cleaner contractual obligation with decreased risk of unintended consequences.

		determines would be reasonable and appropriate to ensure the confidentiality, integrity and availability of the PHI that it creates, receives, maintains or transmits, and provide documentation of such evaluation. 6.2.2 Data Integrity. Each Qualified HIN's security policy shall include the following elements to ensure data integrity of all EHI that it receives, maintains or transmits: (i) Procedures to ensure that EHI is not improperly altered or destroyed; (ii) Procedures to protect against reasonably anticipated, impermissible uses or disclosures of EHI; (iii) Procedures to maintain backup copies of systems, databases, and private keys in the event of software and/or data corruption, if the Qualified HIN is serving as a certificate authority; and Procedures to test and restore backup copies of systems, databases, and private keys, if the Qualified HIN is serving as a certificate authority, to ensure each Qualified HIN can retrieve data from backup copies in the event of a disaster, emergency, or other circumstance requiring the restoration of EHI to preserve data integrity.	6.2.2 We are unclear about the extent to which a QHIN would be in a position to know about inaccurate or unclear data. 6.2.2(iii and iv) – We note that the Draft TEF does not detail a certificate approach. As a result there is no larger context to any requirement in this section specific to certificate authorities. We suggest that ONC work with the RCE in an open process to obtain stakeholder input on an appropriate certificate approach, which then can be outlined in an implementation guide.

		Each Qualified HIN shall report instances of inaccurate or incomplete EHI to the Participant who is the originator of the EHI, and request that Participant remediate such data integrity issues in a timely manner to the extent reasonably possible.	
39	Security	6.2.3 Access Control – Authorization. Each Qualified HIN's security policy shall include the following elements to ensure appropriate access controls and user authentication: **(i)** Procedures to ensure that users attempting to access system functions and EHI possess the appropriate credentials (such as privileges granted and provisioned in security and privacy management) to access the minimum necessary information needed; **(ii)** For SOAP-based transactions, the implementation of the OASIS XSPA Profile of SAML; **(iii)** For SOAP-based transactions, the implementation of the OASIS XSPA Profile of extensible Access Control Markup Language (XACML) Profile for authenticating, administering, and enforcing authorization	6.2.3 Please see the discussion in 6.2 re: this section.

		policies that control access to health information residing within or across enterprise boundaries; and **(iv)** For FHIR APIs-based transactions, the SMART App Authorization Guide for the use of OAUTH 2.0.	6.2.3 (iv) – As stated previously, based on our experience, we do not believe that the TEFCA should provide this level of technical detail. We also do not believe that the focus on OAUTH is applicable for the full range of FHIR-based transactions beyond the individual access use case.
39	Security	6.2.4 Identity Proofing. Each Qualified HIN's security policy shall include the following elements to ensure appropriate identity proofing: **(i)** End Users/Participants. Each Qualified HIN shall identity proof Participants and participating End Users at a minimum of IAL2 prior to issuance of credentials; and **(ii)** Individuals. Each Qualified HIN shall identity proof individuals at a minimum of IAL2 prior to issuance of credentials; provided, however, that the Qualified HIN may supplement identity information by allowing Participant staff to act as trusted referees. Participant staff also may act as authoritative sources by using knowledge of the identity of the individuals (*e.g.*, physical comparison to legal photographic identification cards such as driver's licenses or	6.2.4 (ii) – We ask ONC to clarify if this provision is intended to apply to users/employees or also patients and credentials established for them.

		passports, or employee or school identification badges) collected during an antecedent in-person registration event. All personally identifiable information collected by the Participant staff or Qualified HIN shall be limited to the minimum necessary to resolve a unique identity.	
39-40	Security	6.2.5 Authentication (i) Individuals. Each Qualified HIN shall authenticate individuals at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3. (ii) End Users/Participants. Each Qualified HIN shall authenticate End Users and Participants at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3. (iii) For FHIR API-based transactions the SMART App Authorization Guide for the use of OAUTH 2.0. (iv) For FHIR API-based transactions that require End User authentication, the identity data scopes of the SMART	

		App Authorization Guide for the use of OpenID Connect 2.0.	
40	Security	6.2.6 Credential Management. Each Qualified HIN's security policy shall include the following elements to ensure appropriate credential management: (i) Each Qualified HIN's issuer certificate authorities and registration authorities shall protect repository information not intended for public dissemination or modification. Each Qualified HIN issuer certificate authorities shall provide unrestricted read access to the Qualified HIN's repositories for legitimate uses and shall implement logical and physical access controls to prevent unauthorized write access to such repositories.	6.2.6 – It is unclear to us whether this provision is generally applicable to the QHIN model. More generally, and as noted above, the Draft TEF does not detail a certificate approach, so there is no larger context to any requirement in this section specific to certificate authorities. We suggest that ONC work with the RCE in an open process to obtain stakeholder input on an appropriate certificate approach, which then can be outlined in an implementation guide.
40-41	Security	6.2.7 Transport Security. Each Qualified HIN's security policy shall include the following elements to ensure appropriate data transport security: (i) Authentication Server Requirements. (a) SOAP-based Security. Each Qualified HIN's SOAP-based servers shall conform to the connection authentication requirements as specified in the IHE ATNA Integration Profile for Transport Authentication Security. Each Qualified	

		HIN using local authentication or federated authentication for SOAP-based requests shall convey the locally-authenticated user attributes and authorizations using SAML 2.0 assertions as detailed in the IHE XUA Profile. (b) At a minimum, Qualified HINS shall employ the following ciphers to mitigate the risk of EHI being exposed during transport in order to eliminate all readable EHI that is not encrypted: • Null cipher where encryption is not necessary, but must be configured for the system to work; • Substitution cipher as a minimum cryptographic technique to render EHI unreadable; and • Transposition ciphers or other more advanced cipher techniques to render unsecured EHI information unusable, unreadable or indecipherable to unauthorized individuals. (c) Each Qualified HIN shall ensure that message exchanges are secured using TLS/SSL 1.2 X.509 v3 certificates for authentication, and X.509 certificates are used for authentication of all transactions.	

		(d) FHIR APIs. Each Qualified HIN shall require Participants to conform to the recommendations described in both the Security Considerations sections of RFC 6749 and in the OAuth 2.0 Threat Model and Security Considerations sections of RFC 6819. (ii) Authentication Server Requirements for Third Party Application Access. Each Qualified HIN's security policy that supports third party application access shall implement the following requirements within three (3) months from the date that the Qualified HIN executes an agreement with the RCE; provided, that if the Qualified HIN has not currently implemented FHIR, then the Qualified HIN shall implement the following requirements within twelve (12) months from the date that the Qualified HIN executes an agreement with the RCE: (a) Each Qualified HIN shall support the OAuth 2.0 Dynamic Client Registration Protocol for Individual registration as defined in RFC 7591; and (b) Each Qualified HIN shall authenticate third party applications to the authorization server's endpoint using a JSON Web Token (JWT) assertion signed by the third party application's private key as defined in RFC 7519.	6.2.7 (ii) We do not believe that three months is enough time, to be contractually allocated for any technical change. We also note that there is significant ambiguity around the question of whether or not a QHIN has "implemented FHIR". We suggest that the RCE enlist be given flexibility to obtain input from the implementation community to define realistic timelines.

		(iii) Authorization Server Requirements. Each Qualified HIN’s security policy shall implement the following authorization server requirements within twelve (12) months of the API Implementation Guide being published as specified in Section 2.4 above: (a) Each Qualified HIN’s authorization server shall compare a Participant’s registered redirect universal record indicators with the redirect universal record indicators presented during an authorization request using an exact string match to avoid spoofing; (b) Each Qualified HIN shall ensure that its authorization servers maintain access tokens to single use for a short lifetime of less than ten (10) minutes; (c) Each Qualified HIN shall ensure that its authorization servers use refresh tokens for long term access to the user information endpoint or other similar protected resources; and (d) Each Qualified HIN shall ensure that its authorization servers shall provide a mechanism for the End User to revoke access tokens and refresh tokens granted to a Participant or individual.	

41-42	Security	6.2.8 Certificate Policies. Each Qualified HIN's security policy shall include the following elements to ensure that all Participant SSL certificates meet or exceed the following criteria (i) Key Sizes: - The certificate authority shall utilize the SHA-256 algorithm for certificate signatures; and - All keys shall be at least 2048 bit. (ii) Certificate Authority: - The certificate authority's certificate shall be issued by a mutually trusted certificate authority; and - The certificate authority's certification shall not be self-signed.	We believe these details are best addressed in implementation guides versus the TEF.
42	Security	6.2.9 Policy Binding. Each Qualified HIN's security policy shall include the following elements to ensure appropriate policy binding by associating the X.509 digital certificate to the trust domain by meeting the following conditions: (i) The End Entity certificate possesses a subject distinguished name attribute with a single common name component equal to the fully qualified domain name of the Listed End Point; (ii) The End Entity certificate possesses a subject distinguished name attribute with an organizational unit component representing the trust domain name;	6.2.9 We note that "Listed End Point" is not a defined term in the draft TEF. Generally, as noted above, we suggest that ONC work with the RCE in an open process to obtain stakeholder input on an appropriate certificate approach, which then can be outlined in an implementation guide.

		(iii) The End Entity certificate has at least one (1) subject alternative name extension type of universal record indicator and value representing the trust domain name; and (iv) An approved trust chain issues the End Entity certificate.	
42-43	Security	6.2.10 Auditable Events. Each Qualified HIN shall publicly log the existence of TLS/SSL certificates as they are issued or observed in a manner that permits an audit of the certificate authority. Additionally, each Qualified HIN shall audit the certificate logs to identify the issuance of any suspect certificates. For certificate transparency purposes, each Qualified HIN that acts as a certificate authority shall maintain certificate logs on an ongoing basis. Each certificate log must publicly advertise its URL and its public key via HTTPS GET and POST messages. Each Qualified HIN that acts as a certificate authority shall refuse to honor certificates that do not appear in a certificate log. Each Qualified HIN's security policy shall include the following elements to ensure appropriate auditing: (i) Each Qualified HIN shall generate audit log files for all events. Each Qualified HIN further shall retain all security audit logs (both electronic and non-electronic) and make such audit logs available during any	

		audits. At a minimum, each audit record shall include the following information (either recorded automatically or manually for each auditable event): • The type of event; • The date and time the event occurred; • A success or failure indicator; and (where appropriate) • The identity of the entity and/or operator that was responsible for the event.	
43	Security	6.2.11 Cryptography. Each Qualified HIN shall use asymmetric (*e.g.*, public-key) ciphers for generating secret keys, establishing long-term security credentials and providing non-repudiation services. Each Qualified HIN further shall ensure mutual handshake exchange is based on cryptographic techniques (*e.g.*, TLS 1.2 or above). In addition, members of the trust framework shall deploy a validated cryptographic subsystem consistent with the requirements described in FIPS PUB 140-2. Each Qualified HIN shall ensure that cryptographic modules are validated to the FIPS PUB 140-2 minimum level for the relevant party (or an equivalent protection). Additionally, each Qualified HIN shall apply end-user device encryption standards as adopted in the 2015 Edition final rule. (See §170.314(d)(7)).	

43	Security	6.2.12 IP Whitelist. Each Qualified HIN shall publish and share all IP addresses that are whitelisted. An IP Whitelist can be implemented by the Qualified HIN's end point only if the result complies with the applicable Qualified HIN Participant's non-discrimination policy. For the purposes of this subsection, an end point will be the web service technical URL hosted by a Qualified HIN that is listed in the online TEFCA directory.	6.2.12 – IP Whitelist – We ask ONC to clarify its intention with respect to a QHIN's obligation to "publish" its IP whitelist, which would seem to raise security issues. Further, we question if IP whitelisting is practicable in the absence of a requirement by QHINs to provide each other with an accurate and up-to-date list of IP addresses or ranges in use by that QHIN.
43	Security	6.2.13 Incident Response. Each Qualified HIN who is an issuer of certificate authorities shall maintain backup copies of system, databases, and private keys in order to rebuild the certificate authorities' capability in the event of software and/or data corruption.	6.2.13 – We seek clarification regarding what it means for a QHIN to be "an issuer of certificate authorities". See our prior comments that the Draft TEF does not detail a certificate approach, so there is no larger context to any requirement in this section specific to certificate authorities. We suggest that ONC work with the RCE in an open process to obtain stakeholder input on an appropriate certificate approach, which then can be outlined in an implementation guide.
43	7. Access		
43	Access	7.1 Obligation to Respond to Queries/Pulls. Each Qualified HIN shall respond to all Queries/Pulls by providing all of the EHI in the data classes in the then Current USCDI when and to the extent available, requested and permitted by Applicable Law for the Permitted Purpose of Individual Access, provided that the requesting Qualified HIN has adhered to the privacy and security requirements outlined in Section 6. Notwithstanding the foregoing, a Qualified HIN shall not be required to include individuals as Participants or End Users.	7.1 – We ask ONC to clarify that the Individual Access query would originate from a QHIN Participant and/or one of its End Users. We agree with ONC that the QHIN will not be responsible for directly interacting with individuals. As a practical matter, it's unclear how the responding QHIN would know that "the requesting Qualified HIN has adhered to the privacy and security requirements outlined in Section 6".

43	Access	7.2 Individual Requests for No Data Exchange. Each Qualified HIN shall provide a method for individuals who do not wish to have their EHI exchanged and post instructions on its public website for both recording and communicating such requests to the Qualified HIN at no charge to the individuals. Each Qualified HIN shall process all requests from individuals or from Participants on behalf of individuals in a timely manner and ensure that such requests are honored by all other Qualified HINs on a prospective basis. As a HIPAA Business Associate, the Qualified HIN must also enable a Covered Entity to process the request consistent with the right of an individual to request restriction of Uses and Disclosures.	7.2 –We agree with the concept of allowing a patient to opt out, and this capability follows if a QHIN must maintain a master patient index. As noted above in our comments about the definition of a QHIN, however, it isn't clear that a specific, narrowly defined architecture should be enforced. Generally, this requirement would force a QHIN to have functionality that would more typically reside with one of its Participants or End Users.
44	8. Data-driven Choice	8.1 Population Level Data 8.1.1 Query/Pull: Within twelve (12) months of the standard referenced in 4.1.5 being formally adopted by HL7, the Qualified HIN's Broker shall be able to exchange EHI regarding as many individuals as satisfy the search parameters or are otherwise specified by any requesting Qualified HIN in response to a single Query/Pull. 8.1.2 A Qualified HIN may limit responses to Population Level EHI Queries/Pulls to specific time periods to minimize system disruption due to a lack of	8.1.1 We note that the referenced standard is at 3.1.5 and not 4.1.5 as indicated in the draft text. We point to our comments on the standard at 3.1.5. As a general matter, we ask ONC to define what "adoption" by an SDO means, for example, must it be a normative standard? We note that adoption is really the start of an implementation process and not the end, with the need for pilots that inform further implementation guide revision as needed. 12 months from "adoption" will likely not allow for this process. Overall, there is the need for an RCE-led consultative implementation planning process involving the multiple involved stakeholders. We question the requirement for QHINs to handle any arbitrary search parameters that might be supported by the standard. In education sessions, ONC has indicated that some bases for a query will be permitted, such as *demographics*, but that *condition* would not be an acceptable search criterion. We ask ONC to clarify regarding permitted and excluded search filter criteria.

		bandwidth provided that such limitations are reasonable and do not extend for more than a twenty-four (24) hour period. 8.1.3 Each Qualified HIN must support Population Level EHI Queries/Pulls as described above for all of the Permitted Purposes in accordance with Applicable Law.	We seek clarification regarding the use cases that query initiators actually want to address with this functionality. For instance, will query originators want or always be able to access the full "Then Current USCDI" for every patient that matches the criteria? Or do they need to be able to target specific data elements? We believe the latter is reasonable and is consistent with the general intent behind API access. 8.1.2 We agree with the intent of this provision but ask ONC to clarify that the time periods referenced are the time in which the query must be responded to and not the time period covered by the data. Specifically, we ask ONC to clarify whether the QHIN or its Participants and End Users can apply time bounds to data provided and whether the query initiator can provide such bounds. 8.1.3 – We ask ONC to clarify that Population Level queries cannot be used for Individual Access. Among other issues, such an approach would likely create significant bandwidth issues.
44	9. Participant Obligations		
44	Participant Obligations	9.1 Each Qualified HIN shall be responsible for ensuring that the obligations described in this Section 9 shall be incorporated into all existing and future Participant Agreements.	9.1 – We note that these are very significant requirements and are intended to flow down to end users. As indicated above, we also note that ONC is using Participant Agreement in two senses, QHIN to Participant and Participant to End User.) We ask ONC to work with the RCE to clarify this usage in the final TEFCA. Even used as intended in this section, it appears that the obligations described may not be applicable to the full range of Participant Agreements. For example, if a vendor operates a network with a Connectivity Broker and chooses to become a QHIN, this would make its software license agreements a "Participation Agreement". We ask ONC to clarify if this outcome is the intent. We suspect that the intent of this section, based on our experience, is that Participants must ensure that the flow down terms are legally binding on End Users, not that any current and future contract that is standard among a Participant's End Users needs to include these terms.

	Participant Obligations	9.1.1 Permitted Purposes. Each Participant shall support all of the Permitted Purposes by providing all of the data classes the then current USCDI when and to the extent available when requested and permitted by Applicable Law. Each Participant shall respond to Queries/Pulls for the Permitted Purposes.	
44-45	Participant Obligations	9.1.2 Non-Discrimination. **(i)** A Participant may not require exclusivity or otherwise prohibit (or attempt to prohibit) any of its End Users from joining, exchanging data with, conducting other transactions with, using the services of or supporting any other Participant**.** A Participant shall not unfairly or unreasonably limit exchange or interoperability with any other Qualified HIN or Participant via burdensome testing requirements that are applied in a discriminatory manner, data throttling, or any other means that limits a Qualified HIN or Participant from sending and receiving health information with another Qualified HIN or slows down the rate at which such data is sent or received. As used in this Section 9, a discriminatory manner means action that is taken or not taken with respect to any Qualified HIN, Participant or End User or group of	9.1.2. Please see our applicable Non-Discrimination comments at 5.2.

		them due to the role it plays in the healthcare system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that different treatment shall not be deemed discriminatory to the extent that it is based on a reasonable and good faith belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the Common Agreement (including compliance with Applicable Law) in any material respect. For example, imposing different testing requirements on a Qualified HIN or Participant because it primarily serves providers that are not users of a certain electronic health record system or because it primarily serves payers would be considered discriminatory for purposes of this Section.	
45	Participant Obligations	9.1.3 Privacy. Each Participant agrees to comply with all applicable federal and state laws and regulations relating the privacy of health information	9.1.3 – We agree.
45	Participant Obligations	9.1.4 Identity Proofing. Each Participant shall identity proof participating End Users and individuals in accordance with the following requirements: **(i)** End Users. Each Participant shall identity proof participating End	9.1.4 - The obligations for IAL2 of users would appear to affect/apply to all users who access any health IT systems involved in information exchange. We question whether such a requirement is necessary or realistic.

		Users at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; and **(ii)** Individuals. Each Participant shall identity proof individuals at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; provided, however, that the Participant may supplement identity information by allowing its staff to act as trusted referees and authoritative sources by using personal knowledge of the identity of the individuals (e.g., physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent in-person registration event. All collected personally identifiable information collected by the Participant shall be limited to the minimum necessary to resolve a unique identity and the Participant shall not copy and retain such personally identifiable information.	
	Participant Obligations	9.1.5 Authentication. Each Participant shall authenticate participating End Users and individuals in accordance with the following requirements: **(i)** Individuals. Each Participant shall authenticate participating individuals at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.	9.1.5 – We question whether the required use of these standards is practical.

		(ii) End Users. Each Participant shall authenticate End Users at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.	
45	Participant Obligations	9.1.6 Security Incident and Breach Notification Requirements. Each Participant who is a Covered Entity or Business Associate shall comply with all applicable Breach notification requirements pursuant to 45 CFR §164.402 of the HIPAA Rules. Each Participant further shall notify, in writing, the Qualified HIN without unreasonable delay, but no later than fifteen (15) calendar days after Discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations. Upon receipt of such notice, the Qualified HIN shall be responsible for notifying, in writing, other Participants affected by the Breach within seven (7) calendar days.	9.1.6 - We note that the suggested notification timeframes (15 days/7 days) differ from those broadly supported today. We recommend that ONC work in consultation with the RCE on an incident and breach notification process. We also note also that these timeframes do not meet the more stringent reporting requirements that federal agencies have indicated are necessary to support their participation in the eHealth Exchange.
45	Participant Obligations	9.1.7 Security Technical Requirements. Each Participant shall be responsible for complying with the technical security policy requirements relating to authentication, identity proofing and individual authorization described in Sections 6.2.3 to 6.2.5.	
46	Participant Obligations	9.1.8 Exchange of Data Elements. Each Participant shall be responsible for exchanging data elements, if available, in accordance with the USCDI and patient	9.1.8 - We note that this provision creates substantial data obligations for Participants. We seek clarification of "if available" For instance, does this mean if the information is in the patient record or if it is in the record in standardized and/or structured format?

		demographic data for matching enumerated in Sections 3.2.2, 3.3 and 3.4.	
46	Participant Obligations	9.1.9 Compliance with Applicable Law. Each Participant shall comply with all applicable federal and state laws and regulations.	
46	Participant Obligations	9.2 Participant Compliance. Each Qualified HIN shall be responsible for taking reasonable steps to ensure that all Participants are abiding by the obligations stated in this Section. Each Qualified HIN further shall require that each Participant provide written documentation evidencing compliance with these obligations on at least an annual basis. In the event that a Qualified HIN becomes aware of a Participant's non-compliance with any of the obligations stated in this Section, then the Qualified HIN immediately shall notify the Participant in writing and such notice shall inform the Participant that its failure to correct any deficiencies may result in the Participant's removal from the Health Information Network.	9.2 – We seek clarification regarding whether an enforcement role, if any, is envisioned for the RCE with respect to ensuring that QHINs are taking reasonable steps to ensure that all Participants are abiding by the obligations stated in this Section. We question whether the requirement for annual QHIN compliance documentation regarding Participants will impose administrative burden. We believe that requiring Participants to submit documentation and to have QHINs review such documentation and enforce deficiencies, suggests an accreditation model. We believe this approach would add cost and burden and discourage QHIN participation. In lieu of documentation review, we suggest that the existence of enforceable terms should be sufficient.
46	Participant Obligations	9.3 Failure to Comply with Common Agreement. Each Qualified HIN, each Participant of a Qualified HIN, and each End User acknowledges that the	9.3 - We question whether the proposed compliance approach that is being established on top of a private sector exchange model will keep pace with a rapidly evolving eco-system.

		Recognized Coordinating Entity, other Qualified HINs, other Participants, and other End Users may report any failure to incorporate or to abide by the terms and conditions of the Common Agreement to ONC and/or the Office of the Inspector General, if the Qualified HIN, Participant, or End User has a reasonable belief that the conduct may constitute information blocking (as defined by Section 3022(a)(1) of the Public Health Services Act) or, with respect to a health IT developer, that the conduct is contrary to any condition or requirement of the developer's certification under any program(s) maintained or recognized by ONC. A Qualified HIN's failure to incorporate the Common Agreement's terms and conditions into a Participant Agreement to the extent required herein shall be considered evidence of a material breach of the Common Agreement.	We do not agree that any omitted Common Agreement term, however minor, should be considered a material breach. We recommend a more collaborative approach, which leverages compliance with existing law and regulation, and suggest that the RCE support a required, non-binding dispute resolution process to address disputes and hopefully resolve them before further escalation.
	Participant Obligations	9.4 Incorporation of Participant Obligations. Each Participant shall ensure that the obligations described in this Section 9 are incorporated into all existing and future agreements with the	9.4 - We suggest narrowing the scope of these obligations to the agreements specified in the TEFCA as applying to the TEFCA purposes.

		entities and individuals with which it exchanges information.	
	Participant Obligations	9.5 Compliance with Emergency Preparedness Requirements. Each Qualified HIN and each Participant shall comply with the *Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers as further described in* 81 FR 63859.	We believe that HINs and QHINs which support query-based exchange can be leveraged to support emergency response efforts, such as PULSE.
46	10. End User Obligations	10.1 Each Participant shall be responsible for ensuring that the obligations described in this Section 10 shall be incorporated into all existing and future End User Agreements.	10.1 – As previously indicated, we suggest that ONC define the term "End User Agreement". In addition, we suggest that the terms only apply to future and existing End User Agreements which pertain to the TEFCA.
46	End User Obligations	10.1.1 Permitted Purposes. Each End User shall support all of the Permitted Purposes by providing all of the data classes of the then current USCDI to the extent available when requested and permitted by Applicable Law. Each End User shall respond to Queries/Pulls for the Permitted Purposes.	
47	End User Obligations	10.1.2 Non-Discrimination. An End User shall not unfairly or unreasonably limit exchange or interoperability with any Participant such as by means of burdensome testing requirements that are applied in a discriminatory manner, data throttling, or any other means that limits	10.1.2 – See our prior comments on this issue.

		the ability of a Qualified HIN or Participant to send or receive EHI with another Qualified HIN or slows down the rate at which such data is sent or received. As used in this Section 10, a discriminatory manner means action that is taken or not taken with respect to any Qualified HIN, Participant or End User or group of them due to the role it plays in the healthcare system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that different treatment shall not be deemed discriminatory to the extent that it is based on a reasonable belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the Common Agreement (including compliance with Applicable Law) in any material respect. For example, imposing different testing requirements on a Participant or End User because it primarily serves providers that are not users of a certain electronic health record system or because it primarily serves payers would be considered discriminatory for purposes of this Section.	
47	End User Obligations	10.1.3 Identity Proofing. Prior to the issuance of access credentials by Participant, each End User shall be required to identify proof at Identity Assurance Level 2 (IAL2).	

47	End User Obligations	10.1.4 Authentication. Prior to the issuance of access credentials by Participant, each End User shall be required to authenticate at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.	
47	End User Obligations	10.1.5 Security Incident and Breach Notification Requirements. Each End User who is a Covered Entity or Business Associate shall comply with all applicable Breach notification requirements pursuant to 45 CFR §164.402 of the HIPAA Rules. Each End User further shall notify, in writing, the Participant, if affected by the Breach, without unreasonable delay, but no later than fifteen (15) calendar days after discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations.	
	End User Obligations	10.1.6 Exchange of Data Elements. Each End User shall be responsible for exchanging data elements, if available, in accordance with the USCDI and patient demographic data for matching enumerated in Section 3.2.2, 3.3 and 3.4.	
	End User Obligations	10.1.7 Failure to Comply with Common Agreement. Each Qualified HIN, each Participant of a Qualified HIN, and each End User acknowledges that the Recognized Coordinating Entity, other Qualified HINs, other Participants, and other End Users may report any failure	10.1.7 - We question whether the proposed compliance approach that is being established on top of a private sector exchange model will keep pace with a rapidly evolving eco-system. We do not agree that any omitted Common Agreement term, however minor, should be considered a material breach. We recommend a more collaborative approach, which leverages compliance with existing law and regulation, and

		to incorporate or to abide by the terms and conditions of the Common Agreement to ONC and/or the Office of the Inspector General, if the Qualified HIN, Participant, or End User has a reasonable belief that the conduct may constitute information blocking (as defined by Section 3022(a)(1) of the Public Health Services Act) or, with respect to a health IT developer, that the conduct is contrary to any condition or requirement of the developer's certification under any program(s) maintained or recognized by ONC. A Participant's failure to incorporate the Common Agreement's terms and conditions into an End User Agreement to the extent required herein shall be considered evidence of a material breach of the Common Agreement.	suggest that the RCE support a required, non-binding dispute resolution process to address disputes and hopefully resolve them before further escalation.
48	End User Obligations	10.1.8 Compliance with Applicable Law. Each End User shall comply with all applicable federal and state laws and regulations	