



Elizabeth Hall
Vice President, Public Policy and Issues Management
Anthem, Inc.
1001 Pennsylvania Avenue, NW, Suite 710
Washington, DC 20004
(202) 628-7844

Submitted via email: rce@sequoiaproject.org

September 14, 2021

The Sequoia Project
8300 Boone Blvd, Suite 500
Vienna, Virginia 22182

Re: QHIN Technical Framework (QTF)

Dear Sequoia Project Leads,

Anthem, Inc. (Anthem) appreciates this opportunity to comment on the Qualified Health Information Network Technical Framework (QTF), which lays the functional and technical requirements for Qualified Health Information Networks (QHINs) that participate in the Trusted Exchange Framework and Common Agreement (TEFCA).

Anthem is a leading health benefits company dedicated to improving lives and communities and making healthcare simpler. Through its affiliated companies, Anthem serves more than 117 million people, including more than 44 million within its family of health plans. We aim to be the most innovative, valuable and inclusive partner. We look forward to supporting the ongoing work of The Sequoia Project, as well as the Office of the National Coordinator for Health IT (ONC) and other data exchange stakeholders, to operationalize TEFCA and enhance the value of nation-wide network exchange.

Anthem appreciates the work conducted by The Sequoia Project, ONC's Recognized Coordinated Entity (RCE) to gather standards and technical requirements for QHINs participating in TEFCA, as well as the additional related work on the Common Agreement expedited for release for public comments in the near future. In response to the QTF proposal and opportunity for feedback, we offer the following considerations below.

General:

Anthem applauds ONC and The Sequoia Project's work to build out this common protocol to advance nationwide interoperability and exchange of health information. We agree that "the technical and functional requirements described in the QTF reflect many of the technologies and standards used for network-based health information exchange today." However, in consideration of technological innovations underway and enabling a future-proof nationwide exchange network, we recognize the ability to further this initiative through layering the protocols expertly created by TEFCA-related stakeholders on top of the technological capabilities of blockchain-based technologies. The foundations of blockchain, including but not limited to a distributed ledger, consensus-based protocols, cryptographic security, and data immutability will further promote accurate, safe, and real-time trusted

information exchange across TEFCA participating entities. Anthem recommends expanding the QTF to ensure support of blockchain networks as QHINs and, in response to the comment areas, offers several considerations below.

Definitions:

We first request the QTF to clarify standards and processes around the Enterprise Master Patient Index (eMPI), including protocols for collecting, storing, and managing identifiers, and how this information is updated and how often. This will enable alignment of QHIN practices and help ensure efficiency and accuracy of patient matching across systems. Additionally, under “HomeCommunityID (HCID): A globally unique identifier for an Actor,” we request additional clarification on this definition and its usage, which will help promote uniformity across the QHIN’s implementation and use of the HCID.

QHIN Exchange Scenarios:

Anthem supports the Integrating the Healthcare Enterprise (IHE) standards included throughout the QTF, as they are well vetted and implemented. We encourage continued consensus building, including rigorous processes and considerations when adopting new standards. We also note the overarching query response approach and workflow throughout the QTF and ask the RCE to consider future draft frameworks that include a subscribe and publish model.

Specifically, under scenarios for **message delivery**, the QTF directs each QHIN involved in Message Delivery to “maintain audit logs of all activities and transactions the QHIN performed in the process of delivering the message according to the IHE [Audit Trail and Node Authentication] (ATNA) profile.” Anthem supports the maintenance of audit logs, but we encourage the next update of the QTF consider and support the functions and benefits of blockchain-based technologies for audit log purposes. Blockchain enables the cryptographic securing of all entries into the network. Cryptography ensures the blocks of the chain form a chronological and unbreakable series of transaction data, automatically creating audit logs with timestamps and information on the parties interacting, maintained by security protocols that embed accuracy.

Requirements for Functions and Technology to Support Exchange:

Anthem supports expansion of nationwide data exchange and is in agreement that standards for function and technology will foster sharing arrangements and capabilities between TEFCA-participating entities. In the segments below, Anthem covers blockchain capabilities that meet and exceed these QTF proposed requirements, and requests that the next iteration of the QTF directly support blockchain technology as a method to meet these exchange functions.

First, under **certificate policy**, the QTF proposes that “QHINs must possess appropriate digital certificates for authentication, encryption, and signing. QHIN certificates will be chained to root certificates issued by Certificate Authorities approved by the RCE. The RCE may also establish a broader certificate policy.” Anthem supports the holding of appropriate digital certificates, and we request the RCE to continue its work with stakeholders to further clarify and update certificate policies as needed. Anthem also requests that the QTF support the use of blockchain technology for digital credentials and certificate trust. For example, blockchain can enable interoperability using zero-trust credentials. Under the protocols established by a blockchain network, only verified participants would be able to

participate in any data exchange. Appropriate certifications would be authenticated, encrypted, and signed; and their connection would be directly associated, or rooted, with their appropriate certificate authorities. This would help resolve certification issues and create significant efficiencies over other methods of exchange.

Second, the QTF includes the requirement that QHINs “must provide a **secure channel** to ensure transport-level security for all transactions under their domain.” Blockchain can provide a distributed workflow for identity dispute and error management. The decentralized network of information on Blockchain enables a constantly updated record of truth that follows common agreements and protocols of those connected to the network. Additionally, blockchain allows for increased security by design. As information is not stored or run solely by a central entity, the ability or incentive for hackers to breach an information database can be greatly decreased. Finally, blockchain allows for real-time auditability and pinning of dependencies, or the direct tracing of sources and verifications.. As previously mentioned, data on the chain can be cryptographically secured, which provides high confidence that data cannot be intentionally or unintentionally altered, and if data is accessed or appended, the chain maintains real-time audit logs of all transactions and parties involved.ⁱ

Third, under **user authentication**, the QTF asks that “all entities and persons requested QHIN-to-QHIN exchange must be authenticated and authentication information must be shared ‘upstream’ for access control and auditing purposes.” Under the protocols established by those participating in the blockchain network, only verified participants would be able to access and use the blockchain’s Public Key Infrastructure (PKI) encryption methodology. Under PKI, users on the network have a public key that authenticates their account, which links to a private key that is analogous to their secret password. These keys mathematically prove the user’s control of the information. With the added benefits of zero-trust authentication in blockchain, all users leveraging the network must be authenticated, authorized, and continuously validated for security purposes.ⁱⁱ With this level of security enabled between blockchain networks, we ask the QTF to consider the ability of QHINs to issue “offchain” storage to one another. We ask the updated version of the QTF to consider this as a secure and permissible workflow.

Fourth, specific to **patient identity resolution** requirements, we agree with and support the ability of the QHINs to accurately resolve requests to match patient demographic information with patient identities. We ask the QTF to consider recommendations to update information outside of direct requests if errors in data or wrong matches are identified. We also ask the QTF to enable flexibility for demographic data changes. We also note that blockchain technology can enable the generation of a decentralized identity, which would reduce security risks on a single entity in the network and involve consensus for validating updates across network participants. We request that the QTF terminology, including the eMPI, consider and enable this decentralized nature.

Regarding **performance measures**, the QTF currently calls for data submission to the RCE on a monthly and quarterly basis. As previously described, blockchain technology automatically creates audit logs that include timestamped transactions and information of the parties interacting that are linked and secure along the chain. In place of set performance measurement submissions, the RCE could leverage these audit logs and be ensured of the accuracy of the information provided.

Additional Questions

In the QTF feedback, The Sequoia Project asks commenters to discuss if the QTF should include QHIN message delivery either a) as a requirement, with a future transition to Fast Healthcare Interoperability Resources (FHIR) standards; b) defer message delivery standards until a FHIR standard is readily available; or c) include the IHE Cross-Community Document Reliable Interchange (XCDR) as an option standard until the FHIR standard is ready. Anthem supports the options to defer standards or include as an option until an FHIR standard is fully tested and ready. Requiring a standard with a known short life span does not support innovation and may result in stalled and duplicative efforts for QHIN message delivery.

Additionally, the QTF asks commenters for feedback on what elements should be included in a TEFCAs FHIR roadmap to further support and enable the use of FHIR data by health IT systems. First, we reiterate and strongly suggest that The Sequoia Project and ONC, in and outside of the QTF, continue to support innovation and updates to secure data exchange technologies such as blockchain. We also see the capability and promise for TEFCAs to build out further large-scale information exchanges. However, implementation guides for FHIR bulk transfer are currently not specific enough to define the appropriate themes of consent. Without defining a consent model, implementation becomes expensive and difficult. We recommend TEFCAs-related activities encourage appropriate vetting and finalization of the bulk FHIR implementation guides and refer to related and appropriate population-level data processes in future technical and functional standards documents, as well. Finally, it is known that that not all versions of FHIR are backwards compatible. However, providers and health information exchanges cannot quickly move their data from one version to another. Blockchain technologies are able to address this gap, and will serve not only as an intermediary, but also as a long-term option to efficiently synchronize between networks on differing versions and updates. We suggest exploring opportunities to leverage blockchain technology so health IT networks can more succinctly coordinate network FHIR data exchange.

We value the work of ONC and The Sequoia Project to implement the Trusted Exchange Framework and Common Agreement and related standards and documentation. We welcome the opportunity to discuss our recommendations for the QHIN Technical Framework. Should you have any questions or wish to discuss our comments further, please contact Stephanie Fiore at 667-209-1355 or Stephanie.Fiore@anthem.com.

Sincerely,



Elizabeth P. Hall

Anthem is a leading health benefits company dedicated to improving lives and communities and making healthcare simpler. Through its affiliated companies, Anthem serves more than 117 million people,

including more than 44 million within its family of health plans. We aim to be the most innovative, valuable and inclusive partner. For more information, please visit www.antheminc.com or follow @AnthemInc on Twitter.

ⁱ Vigna, P., & Casey, M. J. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. Macmillan Publishers.

ⁱⁱ Trust No One: The Rise of Zero Trust Networks. (2020, November 16). IoT For All. <https://www.iotforall.com/rise-of-zero-trust-networks>.