CIVITAS
Networks for Health

October 21, 2021

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

Submitted electronically via email to rce@sequoiaproject.org

RE: Elements of the Common Agreement and "Elements of the Common Agreement: Draft QHIN Eligibility Criteria" (released October 7, 2021)

Dear TEFCA Recognized Coordinating Entity (RCE) colleagues,

On behalf of Civitas Networks for Health, we appreciate every opportunity to provide feedback on national interoperability frameworks and approaches like the Trusted Exchange Framework and Common Agreement ("TEFCA"). Civitas Networks for Health is a newly launched organization. The Strategic Health Information Exchange Collaborative (SHIEC), representing 89 health information exchanges (HIEs) and Associate Members, recently joined forces with the Network for Regional Healthcare Improvement (NRHI), representing 29 Regional Health Improvement Collaboratives (RHICs) and Affiliate Members, to form Civitas Networks for Health. Civitas is a nonprofit national collaborative comprised of member organizations working to use health information exchange, health data, and multi-stakeholder, cross-sector approaches to improve health. Collectively, we represent more than 95% of the United States, and we are committed to educating, promoting, and influencing both the private sector and policy makers on matters of interoperability, quality, coordination, health equity and cost-effectiveness of healthcare. We support local health innovators by amplifying their voices at the national level and increasing the exchange of valuable resources, tools, and ideas.

While we recognize that the ongoing development of TEFCA has moved beyond the initial drafts, we would like to direct you to the 2018 comment letter prepared by Civitas' predecessor, SHIEC, and the 2019 comment letter from the Health Information Management Systems Society (HIMSS). We believe that those letters include important perspectives from industry representatives that should be included in future TEFCA development. In particular, they ask that ONC (now in partnership with the RCE) create a nationwide exchange environment where current interoperability and exchange efforts are fully leveraged to achieve the goal of a single on-ramp to connectivity across the country. **Additionally, the 21st Century Cures Act ("Cures Act") provides that efforts must steer clear of disruption of current health information networks. Considering this, we now recommend that ONC and the RCE reach out to key HIE and health system stakeholders to gather specific feedback on this point in order to ensure that the current vision of TEFCA complies with this part of the law.**

Civitas and the specific members who have signed below are happy to provide initial feedback to the "Elements of the Common Agreement" made available to the public on September 20, 2021,

and the "Elements of the Common Agreement: Draft QHIN Eligibility Criteria" released October 7, 2021. Our members appreciate the opportunity to provide feedback via multiple methods—previously, in public and targeted meetings, and here in written form. We are also happy to continue to work directly with you to provide more detailed feedback as the Common Agreement is further developed. Please note that these comments are a reaction to not only the RCE's written summaries, but the subsequent RCE calls devoted to discussing the Common Agreement and QHIN Eligibility Criteria.

1. Exchange Purposes and Required Responses

Civitas supports a contractual framework for exchange purposes that aligns with HIPAA and gives participants at all levels of the TEFCA ecosystem the ability to opt out of particular exchange purposes for which they cannot support due to compliance with applicable laws. It is Civitas's experience that community health information exchanges (HIEs) today are generally structured to support HIPAA-permitted treatment, payment, and limited health care operations, as well as some limited public health use cases. However, the industry is less mature with respect to supporting HIPAA-authorization based use cases (such as Benefits Determinations) and Individual Access Services (IAS). Additionally, many states still impose written consent requirements on the disclosure of health information for non-treatment purposes, including disclosures for payment and health care operations activities. These use cases typically trigger legal issues involving who has the responsibility (and liability) for ensuring compliance with HIPAA authorization requirements (and other state or federal consent requirements), as well as individual identity and authority verification issues.

For instance, the RCE contemplates permitting individuals to use consumer-facing applications owned or offered by entities who will verify the individual's identity and authority. Yet, because many of these applications are not subject to HIPAA, there are not satisfactory assurances that the identity and authority verification measures used will meet HIPAA-required privacy and security standards, which HIPAA covered entity and business associate participants in the TEFCA framework are required to meet to ensure that the access or disclosure is authorized and not a breach. Moreover, delegation of these HIPAA obligations—that is, the responsibility for verifying individual identity and authority—is typically a function that triggers a business associate relationship and requires execution of a business associate agreement (BAA). **We thus seek clarification from the RCE as to whether and how the Common Agreement will flow down BAA requirements to IAS Providers who will perform these functions, and who within the TEFCA framework will be responsible for auditing and monitoring IAS Provider compliance with BAA obligations as part of routine HIPAA risk analyses.**

Because of the practical reality and maturity of existing technical systems—and limitations on the ability to adequately allocate responsibility, risk, and liability under the Common Agreement—we respectfully request that the RCE consider removing the Benefits Determinations and IAS Exchange Purposes from the list of Exchange Purposes for which QHINs, Participants and Subparticipants are required to respond. Rather, these should be Exchange Purposes for which participants in the TEFCA ecosystem may respond. Mandating exchange for the use cases could be reserved for future iterations of the Common Agreement.

Civitas would also like to note that HIPAA does not permit the exchange of protected health information (PHI) among HIPAA covered entities (and their designated Business Associates) for the full range of health care operations activities (as defined by HIPAA), when the entity requesting PHI is doing so for its own its health care operations activities and/or the entity disclosing the PHI is doing it for the receiving entity's health care operations activities. HIPAA limits such exchanges to exchanges among HIPAA covered entities (and their designated business associates) for the purposes listed in paragraph (1) or (2) of HIPAA's definition of "health care operations" or for the purpose of health care fraud and abuse detection or compliance. *See* 45 C.F.R. § 164.506. Yet, the current Common Agreement definitions and proposals for limiting Exchange Purposes based on a user's organizational identity do not seem to account for this.

The RCE should also consider whether administrative and technical infrastructures are sufficiently developed to support a TEFCA Exchange Purpose framework that will require Participants and Subparticipants to identify at the user-level organizational and individual status using a role-based access model that may meet TEFCA needs, but which might not align with the role-based access permissions used internally by these organizations. The RCE might want to consider limiting the Exchange Purposes to what can reasonably be supported by existing infrastructures and role-based access models.

Finally, Civitas seeks clarity from the RCE: Why are Non-HIPAA Entity providers of IAS not subject to mandatory response requirements under the Common Agreement?

2. Participants and Subparticipants

Civitas supports a TEFCA ecosystem that facilitates participation by a broad range of stakeholders that are authorized under federal and state health information laws to have access to health information for legally permissible purposes. The core TEFCA Exchange Purposes—treatment, payment, and limited health care operations—are all limited by HIPAA to those individuals and organizations that qualify as covered entities and business associates and, in some instances, non-covered entity health care providers (as defined by HIPAA). Yet, the RCE proposes to define QHINs, Participants, and Subparticipants as including entities that are not covered entities or business associates. And the RCE does not purport to limit these entities to other entity types that may be permitted access under other HIPAA-permitted use cases, such as public health authorities or entities for which an individual has issued a third-party authorization that would permit the limited access of health information maintained in electronic health records. Expanding participation beyond those individuals and entities that are permitted access under HIPAA may have the unintended effect of undermining the trust framework because there is a lack of certainty regarding the legal authority of entities and individuals who will have access to highly sensitive health information about individuals.

Additionally, the RCE proposes to permit participation by non-U.S. Entities. Non-U.S. Entities may access and store data outside of the United States. This is particularly problematic, as many individuals and entities that exchange health information, including health information of Medicaid and Medicare enrollees, are expressly prohibited from permitting offshore access to the

health information. Moreover, the potential introduction of data into the TEFCA ecosystem that comes from jurisdictions outside of the United States may trigger compliance obligations under non-U.S. laws for which other participants in the system may not be equipped to handle. **Accordingly, we respectfully request that the RCE reconsider the scope of participation in TEFCA.**

3. QHIN Eligibility Criteria

Civitas supports the development of QHIN eligibility criteria that is designed to create a reliable and trusted technical, legal, and administrative framework to support regional and national interoperability in the United States. We strongly support the RCE's requirement that a QHIN applicant demonstrate network governance, and we further suggest that the RCE consider whether that governance model allows for stakeholder input in governance decision at the local and regional levels among Participants and Subparticipants. Civitas further supports the RCE's requirement in the Draft QHIN Eligibility Criteria that all QHINs be U.S. Entities. However, Civitas notes that throughout the RCE's "Elements of the Common Agreement" draft, the RCE provides that under the Common Agreement a QHIN may be a "non-U.S. Entity," *see, e.g.*, page 17 (definition of QHIN). We thus seek clarification from the RCE as to whether, and under what circumstances, a QHIN may be a non-U.S. Entity. Because of the regulatory and legal challenges associated with accessing and storing health information outside of the United States, as well as potential applicability of more stringent non-U.S. laws associated with the exchange of some data from certain jurisdictions, we urge the RCE to limit QHIN eligibility to U.S. Entities.

Civitas further supports criteria used to evaluate technical capabilities to support the exchange of Required Information (RI). However, we seek further clarity on the QHIN eligibility requirement that a QHIN be able "to support" the exchange of RI for all Exchange Purposes. Specifically, is this intended to mean technical support for the exchange modalities (*e.g.*, query or push) or something more? Civitas further requests that the RCE provide guidance on whether it will enter into non-disclosure agreements with applicants to protect the confidentiality of proprietary information required as part of the application process—such as data sharing agreements, operating policies and procedures, financial information, technical infrastructure gaps, and breaches—as well as the extent to which such information may be subject to federal public record requests.

Civitas also understands from the public calls that the RCE is discouraging new market entrants from applying for QHIN status and will require twelve (12) months' worth of high-volume activity on existing networks, in addition to requiring significant financial and administrative disclosures (such as two years of audited financials). Requiring applicants to prove high transaction volumes on a TEFCA network and financial viability for that network going back two years prior to TEFCA implementation poses an interesting challenge, and it may have the unintended effect of reducing innovation and competition at the QHIN-level by significantly limiting the pool of applicants to only those existing networks on which the TEFCA model is being based. **Civitas thus suggests that the RCE clarify that QHIN applicants may meet the 12-month requirement by demonstrating activity among its members, affiliates and/or potential Participants and**

Subparticipants, even if the QHIN entity itself was not incorporated or otherwise formed within that 12-month period.

Additionally, or alternatively, the RCE should consider permitting applicants to demonstrate, via other means, their ability to support high volume activity on the TEFCA network it is requesting QHIN status in order to build and operate. Similarly, other avenues should be available to assess sufficient financial and personnel resources. **In sum, we respectfully request that the RCE consider developing alternative QHIN eligibility criteria that will meet the intended goals—ability to perform, legal structure/governing approach, and resources/infrastructure—while maximizing market participation.**

Civitas also seeks clarification from the RCE on whether and why the 12-month requirement is applicable only to query functionality and not push functionality, or other modes of functionality required by the Common Agreement? Emphasizing one form of exchange over another may again have the unintended effect of discouraging innovation and competition at a time when recently finalized and proposed CMS interoperability regulations are placing an increased emphasis on push functionality (such as admission, discharge, and transfer alerts).

4. <u>TEFCA Information (TI) and Required Information (RI)</u>

Civitas supports the exchange of electronic health information in compliance with applicable laws. As proposed, the Common Agreement will require participants within the TEFCA ecosystem to respond with all "Required Information" (RI). This is currently defined as essentially all ePHI, except for information compiled in anticipation of or use in civil, criminal, or administrative actions/proceedings or psychotherapy notes (as defined HIPAA). However, this contractual requirement does not consider what data elements can be technically supported through the various exchange networks. For instance, it may be technically infeasible for a participant in the TEFCA ecosystem to exchange all RI if the connection at issue, or implementation guide being used, does not support exchange of that data element. **For that reason, we respectfully request that the RCE redefine RI such that it may be limited to those discrete data elements that are supported by the applicable technology being used by that QHIN, Participant or Subparticipant to enable the data exchange.**

Civitas also understands that, under the Common Agreement, QHINs and Participants that facilitate the data exchange network as a service—and as a HIPAA business associate of one another with respect to TI of those individuals for whom a QHIN or Participant might not be functioning as a business associate under its agreements with Subparticipants because those Participants/Subparticipants might not have a relationship with all the individuals for whom they are transacting data across the network—will be permitted to retain and use that TI in accordance with the laws that apply to them. Civitas seeks clarity from the RCE: How will this model ensure that a QHIN and/or Participant that is retaining TI on behalf of another QHIN will not use or redisclose that TI in violation of more stringent laws or business associate limitations (such as no permission to support IAS) that might apply to those QHINs/Participants?

For example, if due to regional laws, QHIN A cannot exchange health information for the full range of HIPAA-permitted health care operations activities without a written authorization, and QHIN A facilitates the push of such information to QHIN C for delivery to QHIN C's Participants' Subparticipants through QHIN B (whose Participants and Subparticipants do not have a relationship with those individuals) pursuant to a written authorization that authorizes the disclosure to those Subparticipants of QHIN C, how will the Common Agreement ensure that QHIN B does not use or redisclose the TI in violation of the individual's written authorization or without the individual's written authorization?

We understand that the RCE intends to require all participants in the TEFCA ecosystem to comply with all applicable laws—including more stringent laws; however, the mechanisms for ensuring this are unclear and may be challenging in situations where the data being retained by pass-through QHINs and Participants is subject to different and inconsistent laws. **The RCE may thus want to consider whether pass-through QHINs and Participants should be permitted to retain TI.**

5. Governing Approach to Exchange Activities Under the Common Agreement

Civitas supports a governing approach that not only solicits participation but also places governance in the hands of the stakeholders that will be participating in the TEFCA framework. **To that end, Civitas respectfully requests that the RCE consider giving the Governing Council greater decision-making authority over which entities will be qualify for QHIN status.**

6. Individual Access Services (IAS)

Required Support for IAS

Civitas supports efforts to improve individual access and control over their health information within the existing federal and state privacy and security framework. As currently envisioned, the Common Agreement will require QHINs, Participants and Subparticipants to support individual access to TI data maintained by that entity. Under the HIPAA compliance framework, whether or not a business associate (such as a QHIN or Participant) can support an individual access use case is determined by the permissions given to them in the HIPAA business associate agreement (BAA). HIPAA covered entity providers and health plans may not be willing to permit third parties to provide (or facilitate) individual access services in the BAA because, for example, the electronic health record (EHR) technology is not yet sophisticated enough to segment data that a provider or plan has determined there is a legal compliance or legally cognizable harm that would result from the access. Consequently, and due to data segmentation infeasibility, the only approach for those data suppliers may be to withhold permission to support an individual access use case. Moreover, there are significant security, technical, administrative, and cost considerations associated with whether the identity and verification processes associated with IAS meet minimum HIPAA privacy and security requirements. IAS Providers that are not regulated by HIPAA may have processes in place that do not meet HIPAA requirements. It is for these reasons that it may be premature to require support for IAS at this time.

IAS Privacy and Security Requirements

Civitas applauds the RCE's commitment to requiring all participants within the TEFCA ecosystem to comply with basic security requirements, such as encryption and security incident notifications. However, the RCE's current proposals for the Common Agreement and SOPs are silent on the minimum identity and authority verification procedures that must be in place to support IAS. These security procedures are critical to any exchange framework that will support IAS. The Office for Civil Rights (OCR) often refers covered entities and business associates to the National Institute of Standards and Technology's (NIST) publications for guidance on the security protocols necessary to meet the HIPAA privacy and security standards. Given the high sensitivity of the health data that will be exchanged through the TEFCA framework, the NIST Digital Identity Guidelines (NIST SP 800-63-3) and subsequent guidance (NIST SP 800-63A and NIST SP 800-63-3) would suggest an Identity Assurance Level of no less than IAL2 be required for IAS Providers.

7. Fees

Civitas supports establishing a TEFCA framework that is marketplace neutral and will support innovation and competition. To that end, the Common Agreement should permit participants that operate within the TEFCA ecosystem at all levels to seek to recover the costs for their services, including a reasonable profit margin, and to be exempt from required data exchange in those instances where the data requestor has not paid a reasonable fee for services. **To promote this innovation and competition, Civitas respectfully requests that the RCE consider neither prohibiting nor endorsing any particular economic model for cost recovery. Rather, QHINs, QHIN Participants and Subparticipants should have the economic freedom to choose their business models**. Prohibiting fees in certain circumstances (where fees would otherwise be permissible under applicable law), and mandating exchange with entities that have not paid for those services, may have the inadvertent consequence of undermining innovation and competition by limiting QHIN- and Participant-level participation among existing marketplace actors whose corporate and financial structures may enable them to offset the true cost of data exchange services under TEFCA through their non-TEFCA, commercial business lines.

8. Standing Operating Procedures

Civitas acknowledges the importance of standard operating procedures (SOPs) in supporting data exchange networks. Civitas understands that the RCE will relegate to SOPs important, substantive requirements, including without limitation dispute resolution, governance, conflicts of interests, QHIN eligibility criteria and security requirements. **Given the substantive importance of these topics, Civitas respectfully requests that the RCE enshrine in the Common Agreement a notice and comment process that will ensure meaningful participation and feedback from both QHINs and QHIN Participants.**

9. Definitions

To the extent the definitions have an impact on the substantive elements of the Common Agreement, we've provided our comments on those definitions in connection with the substantive provisions. In this section, we further note the following:

- **Applicable Law.** The current proposed definition would freeze in time the laws in effect at the time of execution. This aspect of the definition will create at least two problems. First, it will prevent the Common Agreement from staying current with the health information privacy and security landscape, which is under constant change. Second, it will create a situation where the applicable laws may differ depending on when a QHIN signs the Common Agreement. We thus respectfully request that this be changed to the "laws and regulations then in effect and as may be amended, from time to time, and applicable to the subject matter herein."

- **Business Associate and Other HIPAA Terms.** Many terms in the Common Agreement are defined by cross-references to the relevant HIPAA definitions. There is currently a notice of proposed rulemaking (NPRM) to change the HIPAA regulations and the HIPAA regulations will continue to change over time, potentially including regulatory citations. Thus, to the extent the Common Agreement will use terms as defined by HIPAA, we suggest simply including a statement in the definitions section that any capitalized terms that are not specifically defined have the meaning assigned to them by HIPAA.

- **Disclosure and Use.** Because most participants in TEFCA will be HIPAA covered entities and their business associates, we respectfully request that the terms "Disclosure" and "Use"—to the extent it is necessary to treat these as defined terms—have the same meaning assigned to them by HIPAA. We believe that adopting this approach will reduce confusion among participants within the TEFCA ecosystem regarding the meaning of these terms. Alternatively, the RCE should consider whether it is necessary to treat these words as defined terms.

- **HIPAA.** HIPAA should be defined to include subsequent amendments. This is particularly important given the pending NPRM to change the HIPAA regulations.

- **Individual.** The RCE's definition of "Individual" is broader than the definition of this term under HIPAA. For instance, it includes any legal representative who can make healthcare decisions on behalf of person, even if that legal representative is not the person's personal representative with respect to some or all of the health information at issue. That's significant because the RCE defines Individual Access Services (IAS) in relation to this definition of "Individual," but without accounting for the fact that the persons covered by the broader definition of "Individual" may not have the right to access, or to authorize a third party (such as a third-party application) to access, the full scope of TI without a HIPAA authorization. Moreover, as a result of the *Ciox Health, LLC v. Azar*, No. 18-cv-0040 (D.D.C. January 23, 2020) decision, an Individual's (as defined by HIPAA) ability to use a third party directive under 45 C.F.R. § 164.524—that is, exercising the Individual right of access to direct in writing that a covered entity give a third party access to health information without a HIPAA authorization—is limited to that ePHI that is maintained in the "electronic health record" (as defined at 42 U.S.C. § 17921(5)). The TI will include ePHI that goes well beyond what is in a provider's "electronic health record," such as ePHI that comes from claims data supplied by health plans. Because the *Ciox* decision limits the

scope of third-party directives, that avenue for permitting disclosure to third party applications is not available with respect to all the TI. Yet the IAS Exchange Purpose does not seem to account for this. **For these reasons, we suggest that the RCE define "Individual" in accordance with HIPAA and reexamine the IAS Exchange Purpose in accordance with *Ciox* and the sources of TI.**

Thank you for the opportunity to provide feedback on behalf of our organization and members and for your continued commitment to improving interoperability and health information exchange. If you have questions, please do not hesitate to reach out to Civitas's interim CEO, Lisa Bari at lbari@citivasforhealth.org.

Sincerely,

Lisa Bari
CEO (Interim)
Civitas Networks for Health and Civitas Networks for Health Association.

HIE MEMBERS WHO JOIN THIS COMMENT LETTER
Contexture (Colorado Regional Health Information Organization and Arizona's Health Current)
Greater Houston Healthconnect
Midwest Health Connection (Missouri)
Velatura Health Information Exchange Corp (VHIEC)