October 21, 2021

Mariann Yeager
Chief Executive Officer
The Sequoia Project
8300 Boone Blvd.
Suite 500
Vienna, Virginia 22182

Submitted via email to: rce@sequoiaproject.org

Dear Ms. Yeager:

WEDI commends the Office of the National Coordinator for Health Information Technology (ONC) and the Recognized Coordinating Entity (RCE) for the release of the proposed elements of the Common Agreement for the Trusted Exchange Framework and Common Agreement (TEFCA) and for the open and transparent process for development of the TEFCA. We are pleased to offer comments and recommendations on the proposed element of the Common Agreement.

WEDI was formed in 1991 by then Secretary of the Department of Health and Human Services (HHS) Dr. Louis Sullivan to identify opportunities to improve the efficiency of health data exchange. WEDI was named in the Health Insurance Portability and Accountability Act (HIPAA) as an advisor to the Secretary of HHS. Recognized and trusted as a formal advisor to the Secretary, WEDI is the leading authority on the use of health information technology (IT) to efficiently improve health information exchange, enhance care quality and reduce costs. With a focus on advancing standards for electronic administrative transactions, and promoting data privacy and security, WEDI has been instrumental in aligning the industry to harmonize administrative and clinical data.

Overall, WEDI is strongly supportive of establishing a common agreement and set of guardrails for the trusted exchange of electronic health information. TEFCA represents another phase of ONC's efforts to advance interoperability across the nation's health care system in support of the access, exchange, and use of electronic health information.

WEDI commends the work of the ONC and RCE to advance the interoperability of electronic health information. The 21st Century Cures Act pushed for interoperability to be a priority for the industry and TEFCA represents an important step towards achieving this goal. As ONC further develops their approach to advancing interoperability, we encourage the collaboration with the Centers for Medicare & Medicaid Services (CMS), as well as industry stakeholders such as WEDI.

Comments and Recommendations on the Draft Elements of the Common Agreement

RCE proposal: *2. Exchange Purposes. The term Exchange Purposes identifies the reasons for which information could be requested and shared through QHIN-to-QHIN exchange. Initially, QHINs would support the following Exchange Purposes: • Treatment, • Payment, • Health Care Operations, • Public Health, • Benefits Determination, and • Individual Access Services. The Common Agreement would specify the requests, Uses, Disclosures, and responses that would be permitted, prohibited, and required.* (Pages 3-4)

WEDI response: WEDI agrees with the six initial exchange purposes for which information may be requested and shared for QHIN-to-QHIN exchanges. These include treatment, payment, and health care operations (aligning with HIPAA), public health, benefits determination and individual access services.

The draft also indicates the RCE will work with the industry to seek additional exchange opportunities, including biomedical research as one example. On page 6 of the draft Common Agreement, it states "TEFCA Information may also include HIPAA de-identified information." We agree that it is likely that participants will seek to leverage de-identified data and we urge ONC and the RCE to investigate opportunities to exchange de-identified data for public health and research purposes. At the same time, while we agree that new exchange opportunities should be explored, we recommend that the RCE focus first on normalizing the six initial exchange purposes before adding additional purposes. As well, whenever a new exchange opportunity is contemplated, it should be released in draft form with ONC and the RCE permitting the public to submit comments prior to its finalization.

RCE proposal: *The Common Agreement would specify the requests, Uses, Disclosures, and responses that would be permitted, prohibited, and required*. (Page 4)

WEDI response: Regarding the approach to the information exchange between QHINs, Participants, or Subparticipants. as indicated on Page 4 of the Elements of the Common Agreement, the information exchange between above stakeholders assumes Request-Response approach only. Not including alternative approaches, such as Publish-Subscribe, significantly limits the scope of applicable information exchange architectures and opportunities to innovate on the Network to achieve even greater effectiveness and efficiencies. For example, use of Publish-Subscribe model will allow real-time dynamic information updates across all authorized participants without the need for pushing the Requests and pulling the Responses each time information is needed.

We also recommend to explicitly support the employment of new / breakthrough technologies for connectivity and information exchange. This will further foster the innovation on the network while attracting new stakeholders on both supply and demand sides of the ecosystem.

RCE proposal: *11. Privacy and Security. The Common Agreement will promote strong privacy and security protections. Most connected entities will be HIPAA Covered Entities or their Business Associates, and thus already required to comply with the HIPAA Privacy, Security, and Breach Notification Rule requirements. To ensure that privacy and security protections cover certain entities that are not subject to the HIPAA Rules, the Common Agreement would require such Non-HIPAA Entities to protect TEFCA Information that is individually identifiable in substantially the same manner as HIPAA Covered Entities protect PHI, including having to comply with the HIPAA Security Rule and most provisions of the HIPAA Privacy Rule. This alignment will promote trust. QHINs would be expected to meet and maintain third-party certification to an industry recognized cybersecurity framework and undergo annual security assessments. The Common Agreement would require flow-down contract provisions for all Participants and Sub participants to undertake, at a minimum, security measures that align with the HIPAA Security Rule, even if they are not HIPAA Covered Entities or Business Associates. The Common Agreement would also specify expectations for security incident notifications affecting QHIN-to-QHIN exchange that would apply to QHINs and flow down to Participants and Sub participants. These provisions would be designed to avoid conflict with Applicable Law and duplicative notification requirements. The RCE would actively facilitate information security activities, with the support of a Cybersecurity Council drawn from participating QHINs.* (Page 9)

WEDI response: For TEFCA to be successful, we contend that ensuring that the privacy and security of patient information in transit and at rest must be paramount. The HIPAA privacy and security framework has been a fixture in our health care system for more than two decades and patients and other stakeholders rely on HIPAA for the confidence that information is kept confidential. TEFCA must instill that same level of confidence with patients and other participants that the QHINs and other TEFCA entities have proven their compliance with appropriate privacy and security protocols.

For health care data exchange to happen in an interoperable manner as called for under the 21st Century Cures rules, there must be assurance that participants have established a minimum level of privacy and security. We support ONC and the RCE requiring each QHIN within the exchange environment to complete an appropriate and independent third-party privacy and security accreditation or certification.

The ONC and the RCE have also proposed a security incident notification process. We agree that this process must be in place as TEFCA goes live. Participants must be required to report designated types of security incidents, including ransomware and other cybersecurity attacks. We also recommend that the entity experiencing the security incident be required to document how they identified the incident, how data and or operations were impacted by the incident, and the steps taken to mitigate the impact of the incident. This expanded level of transparency will serve to increase the trust that participants have in TEFCA and will also serve to educate participants and decrease the chance that other entities will experience similar security incidents.

In addition, annual security assessments are proposed in the draft Common Agreement. We concur that these assessments must take place and must be done on at least an annual basis. As we have stated, participant trust that information exchange is being done within an appropriate privacy and security framework is critical. These annual assessments will foster increased trust between the entities sharing data.

The ONC and RCE are also proposing to establish a Cybersecurity Council "drawn from participating QHINs." While we strongly support the creation of a Cybersecurity Council, we do not believe the Council should be comprised solely of participating QHINs. In addition to participating QHINs, the Council should include independent privacy and security experts and well recognized representatives from national health care privacy/cybersecurity initiatives and organizations such as the Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Office for Civil Rights, WEDI and others that could serve to review incidents and provide impartial recommendations to Council members.

WEDI comments on patient matching

QHINs and other TEFCA participants will face a significant challenge accurately identifying the patient during the information exchange process. With the current absence of a national patient identifier, the industry has had to rely on various strategies and algorithms to minimize the chance that a record will be matched with the wrong patient, or a record will fail to be correctly matched to a patient. Improving record matching efforts can directly impact patient care, including, as the Pew Charitable Trust has effectively articulated, during the current national pandemic.[1]

We strongly recommend TEFCA should support the emerging body of work leveraging federated digital identity management. An important CARIN white paper lays out a vision of moving forward in health care leveraging state of the art standards for establishing and sharing digital identities for patients and consumers.[2] Such a vision is already playing out with the issuing of digital driver's licenses in a number of states. We recognize that it will take time to instantiate broadly such a vision. During such time as it takes for a better system to be established, the industry must rely on patient matching methods based upon algorithms. That being the case, WEDI recommends the following actions be taken to improve patient record matching:

- Establish a collaborative process that permits the QHINs and other appropriate TEFCA stakeholders to discuss patient matching challenges and solutions. This collaborative process could involve the creation of a council or committee that would facilitate the identification of best practices related to patient matching solutions.
- Develop pilots of one or more of these identified best practices.

[1] Better Patient Identification Could Help Fight the Coronavirus | The Pew Charitable Trusts (pewtrusts.org)
[2] https://www.carinalliance.com/wp-content/uploads/2020/12/LPCA_CARIN-Alliance-Federated-Trust-Agreement_FINAL-12.3.2020.pdf

- Consider establishing a floor for error matching rates. Once QHINs and other participants meet the "floor," permit entities the flexibility to determine what solution works best for them.
- Explore incorporating standardization of expanded patient demographic data. For example, incorporating a standardized approach to an individual's address would reduce matching errors. We also note that certified EHRs are currently required to capture demographic data such as name, birth date and sex. However, many health records contain other demographic data routinely collected that are not typically used or made available to match records, such as email addresses. Matching rates could be significantly improved by including information such as email address, mother's maiden name or insurance policy identification number—that QHIN technology could use for matching. We urge you to review the work of the Project US@ initiative as you explore patient matching improvement opportunities.

We appreciate the opportunity to share our perspectives regarding the draft Elements of the Common Agreement put forward by ONC and the RCE. Exchanging data in a standardized and efficient manner will result in patients, providers, health plans, and other stakeholders receiving better data, faster. We appreciate your commitment to solicit public input on this important initiative and your willingness to engage directly with the WEDI community. We look forward to continuing to work with ONC and the RCE to educate the industry as the TEFCA process moves forward. Should you have any questions regarding this letter, please contact Charles Stellar, WEDI President and CEO at cstellar@WEDI.org.

Sincerely,

/s/

Nancy Spector

Chair, WEDI

cc: WEDI Board of Directors