KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

October 21, 2021

Mariann Yeager, CEO
The Sequoia Project/RCE
8300 Boone Blvd Suite 500
Vienna, VA 22182
Mariann.Yeager@sequoiaproject.org

**RE:** Response to Request for Comments on the Draft Common Agreement

Dear Ms. Yeager:

Kaiser Permanente shares the goals of simplified connectivity and universal interoperability that the Common Agreement (CA) aims to achieve. We appreciate the opportunity to offer feedback.

**General Comments**

Kaiser Permanente agrees with ONC and its RCE that the CA should build upon the successes of existing network capabilities and infrastructure. We are concerned, however, that the added layer of QHINs on top of existing HIEs and EHRs may make data exchange more cumbersome and expensive, especially for smaller organizations – thus discouraging their participation. We urge the RCE to ensure that the CA elements simplify, enhance, are consistent with, and build upon existing capabilities and requirements related to health information exchange, and provide flexibility for QHINs, Participants and Sub-participants to meet their business obligations in the least burdensome manner.

We believe that the CA should address patient matching and identify proofing. It will be critical for the CA to define the parameters by which patient matching will be performed within a QHIN and between QHINs. Equally important is identity proofing. While it is expected that identify proofing will be required to be performed by the Participant and Sub-participants, the CA also should address it at the QHIN level for QHIN-to-QHIN exchanges, as well as in the Standard Operating Procedures for QHINs.

Further, while we appreciate the opportunity to provide feedback regarding the terms and definitions that the RCE plans to include in the CA, we believe it is equally important to review and provide feedback regarding the minimum terms and conditions that the CA will require to be included in the flow down agreements between QHINs and Participants, and between Participants and Sub-participants. For example, it will be important to address secondary use of

data between and among QHINs, Participants (including participating HIEs/HINs) and Sub-participants to ensure that the data is used in accordance with HIPAA requirements and patient expectations. QHINs and HIE/HINs should not be permitted to make secondary use of data supplied for another purpose (e.g. treatment, payment and health care operations) for commercial gain or other private benefit of the QHIN/HIE/HIN or any other party without express consent/authorization from the entity that supplied the data and from the individual who is the subject of the data.

We look forward to the opportunity to review and comment on these minimum required terms and conditions soon.

We understand that in the TEFCA framework envisioned by ONC and the RCE, there will be at least three levels of contractual engagements covering the end-to-end exchange of information: 1) the Common Agreement to be signed between RCE and QHINs (subject of this request for comments); 2) A Data Sharing Agreement between QHINs and Participant Organizations; and 3) An Information Sharing Agreement between a Participant Organization and one or more Sub-Participant Organizations. We believe it will be beneficial to consider developing and offering a model data sharing agreement and information sharing agreement, to help understand the specific flow down required terms and conditions requirements and other expectations for QHIN participants and sub-participants.

Our specific feedback on CA elements is provided below and based on our past and current experiences with existing vendor agnostic exchanges, which amounted to over 28 million exchanges in 2020 alone.

**Elements of the Common Agreement:**

1. *Definitions*
   No comments

2. *Exchange Purposes*
   <u>Requests</u>
   It is important to distinguish a QHIN's role in trust arrangements, directories, and record location services from its role as a message broker in the middle of EHI-sharing transactions. The former may be necessary and helpful, but the latter may be unnecessary, complex, burdensome, risky, and costly. To promote administrative efficiency and simplicity, we recommend that the CA explicitly permit Participants and Sub-participants to perform data exchanges directly between them instead of going through the QHIN – whether exchanges between two or more Participants and Sub-participants within a QHIN, or exchanges across QHINs - as going through the QHIN would add an additional layer of unnecessary process and interactions with attendant costs, burdens, and risks. The QHIN can receive requests for information about location for an exchange and reply with information from directories about where to submit the query, but, when point-to-point exchange capability exists the query itself and the possible clinical information access or exchange must not necessarily need to go

through the QHIN. Furthermore, in applicable instances, Participants and Sub-participants should be able to directly query each other to obtain directory information.

The CA provides that a QHIN, Participant, or Sub-participant may only request, use, or disclose TEFCA Information for a specific exchange purpose if the QHIN, Participant, or Sub-participant is the type of person or entity that is described in the definition of the applicable exchange purpose. For example, only a health care provider as described in the definition of Treatment could request information for the Exchange Purpose of Treatment. We recommend that the CA provide clear descriptions and examples of which types of individuals or organizations can perform which types of transactions for which type of purposes.

Uses and Disclosure

We agree that the uses and disclosure should adhere to CA privacy and security requirements along with any applicable privacy and security legal requirements. Additionally, we strongly urge RCE to prohibit QHINs from making secondary use of data supplied for another purpose (e.g. treatment, payment and health care operations) for commercial gain or other the private benefit of the QHIN or any other party without express consent/authorization from the entity that supplied the data and from the individual that is the subject of the data. Health data, particularly identifiable data, is inherently sensitive and we are concerned that commercialization of health data will increase consumer mistrust and discourage participation in interoperable frameworks that may help improve population health and reduce health disparities.

Responses

We agree that responses may not be required by the CA in certain situations, however, for requests to governmental agencies that determine non-health care benefits that fall under treatment, payment or health care operations under HIPAA and are permitted by applicable law, the response from the agency should be required by the Common Agreement.

We also recommend clarifying that Individual Access Service (IAS) providers are required to respond to queries if the patient opts into sharing their data. Patients should have greater control over how and when their data is used, especially if they would like it shared to facilitate care or payment for services. Additionally, we believe third party apps that access data under the IAS purpose should be held to strict privacy and security controls to protect patient data confidentiality and maintain consumer trust. However, we are concerned that existing applicable law does not extend these privacy and security controls that apply to Covered Entities and business associates under HIPAA to IAS providers. This makes enforcement of violations difficult even if the CA imposes contractual privacy and security requirements. We urge the RCE to consider enforcement mechanisms for non-covered entities including those not subject to the scope of FTC regulatory authority as they define how IAS providers will interface with QHINs, Participants and Sub-participants and receive, maintain and use identifiable health information.

3. *Participants and Sub-participants*
   No comments

4. *Required Flow-Down Provisions*
   We urge ONC and the RCE to publish soon the detailed list of required flow-down provisions for review and comment by the industry, along with any additional minimum required terms and conditions that Participants and Sub-Participants will be expected to perform under a QHIN Agreement.

   We also recommend that the flow-down provisions of the CA specify that TEFCA Participants and Sub-participants are permitted to participate in other networks to which TEFCA exchange provisions do not apply. This will ensure that application of the TEFCA requirements are not exclusive, unduly burdensome or restrictive, or disruptive to existing networks and exchange operations.

5. *TEFCA Information and Required Information*
   We support the recommendation to extend HIPAA requirements to health care providers that are not Covered Entities and that choose to participate in TEFCA. Additionally, we recommend that the CA extend HIPAA requirements to all other non-health care providers that are not Covered Entities as well, for example QHINs and Participants.

   We also recommend that the CA align the definition of Required Information with other law and regulatory requirements applicable to Participants and Sub-participants. For example, in the QTF, required information is limited to the original Common Clinical Data Set (CCDS) and the new US Core Data for Interoperability (USCDI), and not electronic protected health information (ePHI) nor the electronic designated record set under HIPAA. We also recommend that TEFCA include implementation guides to assist QHINs, Participant and Sub-participants in determining the payload for the different use cases. For example, under HIPAA we are only permitted to send the "minimum necessary" data for almost all uses cases outside of Treatment, such as payment or health care operations, and as such sending the entire USCDI might be overinclusive and inappropriate for some of these non-Treatment use cases.

   It will also be important to clarify the intent for, and implications of defining "TEFCA information" to include other information beyond health information. It is not clear what other non-health information would be able to be exchanged via TEFCA, and still be related to the six priority areas.

6. *Governing Approach to Exchange Activities Under the Common Agreement*
   As the governance approach to exchange activities under the TEFCA will be complex, we recommend that the RCE establish a complete Governance Framework that defines in

more detail what bodies will be established to advise and govern TEFCA, to ensure transparency, openness, appropriate representation, good governance practices, and efficiency. In particular, we recommend that Participants and Sub-participants be provided a method independent of QHINs to participate in TEF governance to ensure a balanced representation of all stakeholder interests. Participants and Sub-participants are stakeholders in TEF and will be directly impacted by CA requirements, particularly the required flow downs. It is critical that Participants and Sub-participants are able to engage in TEF governance processes independent of any associated QHIN to ensure that their concerns and recommendations are heard and considered. An approach where Participants and Sub-participants must be appointed by QHINs runs the risk of stifling useful viewpoints and discouraging full participation by all impacted entities.

7. *QHIN Designation and Eligibility Criteria*
   QHINS that store clinical information in document or discrete repositories should be subject to robust security requirements using the NIST security framework, aligned with industry accepted practices to safeguard against ransomware or other cyber-attacks. In addition to requiring the same level of security specifications and controls imposed by HIPAA on covered entities, system and organization controls (SOC 2) audits should also be required for QHINs based on AICPA trust services criteria for security, availability, processing integrity, confidentiality, and privacy. QHINs should also be required to report their cybersecurity risk using the SOC for Cybersecurity framework. SOC2 reports, along with SOC for Cybersecurity reports, should be freely available to QHIN customers and stakeholders.

8. *Cooperation and Nondiscrimination*
   We are strongly supportive of the CA addressing cooperation. There are different layers involved in QHIN exchanges and from a troubleshooting perspective it can be difficult to identify which entity is on point to resolve an issue and how to engage with that entity. We recommend establishing clear guidance on the process for troubleshooting across and within QHINS and possibly setting explicit service level agreements. To promote trust and to support openness, transparency, non-discrimination, and fairness in TEFCA technical requirements we recommend that with regard to TEFCA standards, specifications, and implementation guidance applicable to Participants and Sub-participants the CA should refer to or incorporate either applicable requirements of the National Technology Transfer and Advancement Act (NTTAA) and Revised OMB Circular A-119, or the principles of the WTO Technical Barriers to Trade (TBT) Agreement. Additionally, we recommend that the CA include additional detail about the expectations for information sharing, particularly around cybersecurity risks, threats, vulnerabilities, attacks, etc., as well as how to handle and report data breaches between entities within a QHIN or across multiple QHINs (or by the QHINs themselves).

9. *RCE Directory Service*

   As we mention earlier in response to element 2, we recommend that the CA explicitly permit Participants and Sub-participants to directly query each other to obtain directory information without limitation in order to promote administrative efficiency, simplicity and cost savings.

   We also recommend that CA be more specific about what data is going to be in this Directory Service, what will be the source(s) of the data, how is the directory going to be maintained, who has access to it, how it is secured, and what are the permitted purposes of its use.

10. *Individual Access Services (IAS)*

    We appreciate the emphasis on protecting the privacy and security of individual's health information, however we have concerns with the CA specifying additional privacy and security requirements that will apply to IAS providers. It is important that QHINs, Participants and Sub-participants be governed by privacy and security requirements that are robust, clear and consistent throughout TEFCA and with external requirements. We are concerned that an additional layer of requirements may create conflicting or duplicative requirements for entities that are Covered Entities or business associates under HIPAA. Instead, we recommend that the CA ensure security and privacy requirements are tailored to apply to entities acting solely as IAS providers to ensure uniformity and avoid confusing and duplicative requirements for IAS providers that are Covered Entities and business associates under HIPAA. For example, Covered Entities are required to comply with individual access requests by HIPAA. We recommend that the CA clarify that Covered Entities are not considered to be acting as an IAS under the CA when they are merely complying with individual access requests under HIPAA.

    We understand the desire to recognize individual rights with respect to data maintenance and sharing. However, we are very concerned with the CA requirement that allows individuals to request IAS providers to delete their individually identifiable information maintained by the IAS provider. Many IAS providers are HIPAA Covered Entities and need complete data sets in order to provide treatment or provide payment or conduct health operations. This provision establishes a new privacy policy by contract which may contravene applicable law. We recommend that the CA clarify that it is governed by individual data privacy rights established under state or federal law and that the right to delete may apply only when it has been established by applicable law. Additionally, we recommend that the CA align the request requirements and exceptions among QHINs, Participants, Sub-participants and IAS providers to ensure that entities that meet multiple definitions (e.g. a Participant that is also an IAS) are not subject to operationalizing multiple sets of response requirements and exceptions.

Lastly, we request that the CA align the elements of the IAS privacy notice with existing privacy notice requirements applicable to HIPAA Covered Entities and business associates to ensure that the IAS privacy notice is not duplicative or inconsistent with other privacy notices applicable to the transaction.

11. *Privacy and Security*

We strongly agree with the CA provision to require non-HIPAA entities to protect TEFCA information that is individually identifiable in substantially the same manner as HIPAA Covered Entities and Business Associates are required to. However, in some circumstances Participants or Sub-participants may have security obligations that are outside of or extend beyond HIPAA, for example DoD CMMC level 3 security requirements or marking Confidential Unclassified Information (CUI). It would be helpful if the directory indicated the specific type and level of certification/security that the entity has achieved. This would allow entities with higher levels to tailor their exchanges accordingly.

We urge the RCE to ensure that any reporting requirements regarding TEFCA Security Incidents add value, particularly with respect to entities that already have independent breach reporting obligations under applicable law, and are feasible to implement. The definition of TEFCA Security Incident does not distinguish between TEFCA Information (TI) while it is in transit among QHINs, Participants and Sub-participants pursuant to Framework Agreements, and TI at rest that has been incorporated into an entity's records and that may subsequently be transmitted outside of the TEFCA ecosystem. In the latter case, TI may not be discernable from other information, like PHI, and the entities involved may already be subject to statutory or regulatory breach notification requirements applicable to the TI; e.g., HIPAA breach notification requirements for HIPAA covered entities and business associates and FTC Health Breach Notification Rule. It would be beneficial to require reporting under the CA by entities that store TI if they feasibly can and if they are not otherwise subject to notification obligations under applicable law; e.g., QHINs, HIEs and HINs. We recommend that with respect to other entities, TEFCA Security Incident reporting obligations align with Adverse Security Event notification requirements in the Data Use and Reciprocal Support Agreement (DURSA) and only apply to security incidents involving content that is in the process of being transacted pursuant to Framework Agreements. We believe this approach is industry standard for HIE.

Also, since TI is inclusive of non-health information, it will be important to establish requirements, including obligations with respect to TEFCA Security Incidents, applicable to such information.

We also recommend that the CA include additional provisions to assure the security and integrity of TEFCA data. Specifically, QHINS should not be permitted to combine/consolidate data from multiple sources unless original source provenance can be retained and authenticated indelibly, such as by sending underlying source documents, nor should they be permitted to break open the integrity of a digitally signed document or message or extract, manipulate, or disaggregate individual data elements for any purpose without specific individual consent or authorization for each case. Without an authentic chain of custody that provides objective evidence of original authorship and data provenance, the integrity of health data could be undermined or open to question. Also, it is difficult to determine if or when needed data de-duplication or reconciliation is precise and reliable. These scenarios carry risks, including potential liability for source and receiving entities, other legal and compliance issues, misattribution of provenance, as well as significant privacy risks.

12. *Special Requirements (including Consent)*

As we note above in response to element 10, many IAS providers are also HIPAA Covered Entities and imposing additional consent requirements is administratively burdensome, duplicative, and potentially conflicting with existing laws and regulations that do not require consent for certain purposes (such as treatment). We recommend clarifying that the IAS consent requirements only apply to IAS providers that are not HIPAA Covered Entities.

Additionally, we have concerns with the commercialization of health data due to its inherently private nature. Robust and secure health data exchange is foundational to promoting population health and public trust. As such, we believe QHINs should not be formed solely to commercialize or otherwise enable the sale of health data for the private benefit of any party. Patients should control whether or not their data is sold and QHINs and IAS providers should seek explicit consent prior to commercializing the data, it must never be the default. Also, such consent notices should be specific and limited in duration and purpose. Global consents should be prohibited as well as any consents that purport to apply to future exchanges/QHINs.

13. *Fees*

We agree that the CA should include a provision that prohibits QHINs from charging fees to other QHINs with respect to activities under the CA. However, this does not address affordability for QHIN Participants and Sub-participants. We are concerned that it may become inordinately expensive for entities to participate in QHINs and especially that the expense may deter small organizations. We recommend that the CA include provisions to address the fees that QHINs may charge Participants and Sub-participants to ensure that the fees are reasonable and do not discourage participation. Additionally, we recommend that the CA explicitly permit Participants and Sub-participants to

connect directly, not through a QHIN, when the capability exists and it is a directed request. These types of direct interactions should not incur fees from the QHINs.

14. *Attachment 1 – Standard Operating Procedures*
    We recommend that the CA include a specific SOP for cross-QHIN/Participant/Sub-participant troubleshooting including service level agreements (SLAs) and patient identity management when queries are unsuccessful.

Please feel free to contact Jamie Ferguson (415.250.0561; jamie.ferguson@kp.org) or Zach Gillen (510.418.7438; zachary.m.gillen@kp.org) with any questions or concerns.

Sincerely,

Jamie Ferguson
Vice President, Health IT Strategy and Policy
Kaiser Foundation Health Plan, Inc.