601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004

T 202.778.3200
F 202.331.7487
ahip.org

October 21, 2021

Submitted via email to: rce@sequoiaproject.org

The Sequoia Project
Attention: Mariann Yeager
8300 Boone Blvd.
Suite 500
Vienna, VA 22182

Re: Proposed Elements of the Common Agreement

Dear Ms. Yeager:

AHIP[1] appreciates the opportunity to submit comments in response to the proposed elements for the Common Agreement component of the Trusted Exchange Framework and Common Agreement (TEFCA). Our comments also address the Qualified Health Information Network (QHIN) Eligibility Criteria that were recently released for review and public input.

We are excited to be part of this transformative work within the healthcare sector. AHIP has been working for many years to help the industry realize an interoperable health system that is designed with individual consumers at the center. We look forward to working with your organization in its capacity as the Recognized Coordinating Entity (RCE) and other stakeholders over the next several months as a variety of TEFCA components are put into practice by a variety of entities. Working together, through a public-private partnership, we hope to set baseline legal and technical requirements for secure information sharing on a nationwide scale.

Likewise, we hope to help promote the public initiatives of interoperability and better information transparency that the U.S. Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology (ONC) is overseeing in the regulatory context for providers and Certified Electronic Health Information Technology (CEHRT) and the Centers for Medicare & Medicaid Services (CMS) is overseeing with regards to health care and health insurance providers. We also await the HHS Office for Civil Rights (OCR) regulations to help promote better care coordination and access for individuals to their health

information. The variety of these initiatives will converge to promote better information access and improve care delivery and outcomes for individuals.

We envision a national, interoperable network that is safe and secure where payers need not execute different agreements with each and every stakeholder with whom they wish to exchange information and can seamlessly share data for the purposes of improved transparency, outcomes, efficiency, and affordability. Privacy and security are integral for individual consumers and other entities to trust the processes. Consumer protections should be enhanced through TEFCA and where possible in the Qualified Technical Framework (QTF) and the Standard Operating Procedures (SOPs).

Our comments are designed to address a number of outstanding points which require clarification or to address circumstances in which the existing work streams have prompted questions and differing interpretations. Where possible, we offer our recommendations and positions for improving the work issued to date, understanding that future collaboration will be critical in order to achieve overall success of these initiatives. We appreciate your willingness to work with us and other stakeholders. We stand ready to help inform this important work.

While we welcome the opportunity for stakeholder engagement throughout this process, however, given the quasi-regulatory nature of this activity, the 30-day deadline to prepare comments for this foundational component is concerning. We hope and expect that there will be ongoing opportunities for iterative feedback as this work proceeds. We look forward to future public forums to discuss needed updates, new ideas and revised or new processes to help transform and solidify new procedures for electronic health information.

In concept, we view your work as building “a hub and spokes” model for data exchange similar to the infrastructure on which other industries (e.g., airlines, energy suppliers, transportation networks) base their products and service delivery to individual consumers. As TEFCA information extends beyond the present structure, we ask your organization to continue discussions with stakeholders to determine, as well as monitor, future opportunities and potential risks related to the exchange of combined health information. Privacy, security, and cybersecurity protocols are ongoing and new threats continually emerge. We realize that there will be milestones to celebrate and challenges in the months ahead, but we reiterate our commitment to the project’s goals and collaboration between public and private that seek to use these processes.

Our comments below in Attachment A will address more specific details that correspond with the 13 Proposed Elements in the Common Agreement (CA). We believe the following overarching concepts and key priorities should be stated at the outset:

- **The Overall Contracting Process.** At present, specific legal language of the CA is not publicly available. Lawyers will want to review the specific contractual language that will be in effect for entities that want to voluntarily participate in these processes. Likewise, contractual provisions that will need to "flow down" to Participants and Sub-participants in the TEFCA processes need to be succinct, clear, and realistic in order to garner robust participation.

  This public release of CA Elements begins an initial phase of establishing general parameters and working definitions. However, the minimum required terms and conditions that are to be included in separate data sharing agreements that QHINs will require from their Participants need to be reviewed and vetted, and Sub-participants will need to review contract language to assess if they are ready or must take additional steps to be able to enter into information sharing agreements. As these specific details and contractual provisions remain unknown, required terms and conditions have yet to be determined. Budgets, action plans, and other preparatory measures are unlikely to advance without this critical information.

  We believe making the actual contract language available for public vetting will help expedite the creation of a "boilerplate" contract that can be used without negotiation and amendment to set the framework for the roles and responsibilities of each entity. In addition, creating a visual graphic to educate the public and entities about the definitions, functions, and contracting relationships between and among them (i.e., whether they are a QHIN, Participant, or Sub-participant) with the functions, expectations, and planned information flows would be very helpful.

- **The Application of Laws and Regulations.** Within healthcare, entities face competing compliance obligations and continually make determinations about when and which federal and state requirements apply to a specific situation. For example, many State laws restrict sharing genetic information, HIV-status, and other sensitive health categories. This could mean, for example, that those data could be requested and, in some jurisdictions, cannot be sent. Federal regulations apart from HIPAA have rules for the confidentiality of substance use disorder records (known

as the 42 C.F.R Part 2 regulations or the "Part 2 rules"). Public health benefits contracts (e.g., Medicare Advantage, Federal Employee Health Benefits Program, Medicaid, TRICARE/CHAMPUS) often enumerate specific parameters for information protections, uses, and disclosures. These requirements create additional restrictions applicable to requested data and, if they are sent as part of the TEFCA processes, could raise compliance issues due to a conflicting law or contractual requirement.

The CA will specify the requests, uses, disclosures, and responses that would be permitted, prohibited, and required provided they do not conflict with or would be preempted by applicable laws and regulations. Stakeholders could benefit from clarity on these issues to better understand what support will be made available to help make such decisions, what, if any, contractual restrictions entities and individuals should expect to enact for the information exchanges, and any remedial actions that could affect ongoing operations and contracting status under TEFCA.

We recommend that no entity acting in good faith be penalized for adhering to compliance obligations. In the months ahead, decisions will need to be made about when and what law or regulation applies, in addition to the contractual provisions. We encourage a good faith oversight and compliance approach as opposed to a focus on penalties, fines or terminated contracts for correctable situations.

- **Consent.** Consent is one of the key focus areas. The role of consent processes for parents, guardians, caregivers and others involved in an individual's care merits clarification. Accessing health care services is often done with the help of family members, friends and others. We need to prioritize the needs of individual situations and recognize that while a nationwide exchange is being established, the needs of an individual cannot be overlooked. Individual needs should be accommodated to create access and not to erect not barriers to health care services. For example, situations of information access related to an individual's disability, incapacity, severe illness, guardianship or parental rights can be complex. We recommend that significant details be released which include the substantive elements, technical processes, and overall policies that will govern the consent processes and individual needs.

Because consent is often confused with or can be intertwined with the authorization process under HIPAA, more education about these requirements and whether or not they can be combined in the health information exchange will be essential for individuals' and entities' understanding of these terms and processes.

- **Privacy, Security and Apps.** For many years, AHIP has advocated for bringing third-party application developers and other non-HIPAA entities under the same or similar privacy and security requirements that today apply to HIPAA covered entities when those organization are in possession of individual health information. While the CA intends to use HIPAA privacy and security as the standards for operations, it remains unclear whether a contractual expectation will provide sufficient data security and confidentiality when the contracting entities are unaccustomed to implementing privacy and security parameters based on HIPAA.

  New projects often allow for a testing timeframe or rollout-period for "lessons learned," so that adjustments can be made to better achieve compliance. With the launch of the TEFCA processes, there is no opportunity to have a launch-assessment-and-relaunch process for privacy and security. In other words, entities need to be able to assure individuals, the RCE, and other participating entities that there will be no gaps in privacy and security. In the electronic environment, a vulnerability in any one QHIN, Participant, or Sub-participant can result in a major incident or breach for any other entity or individual.

  While we do not want to deter entities from becoming a Participant or Sub-participant, we need to ensure that individuals' information will be protected by all involved entities using the HIPAA rules and ensuring that no part of the process poses a significant risk to privacy, security or cybersecurity. Any entity that is part of this process must be privacy, security, and cybersecurity-ready from day one.

- **Patient Identifiers and Identity Proofing.** There is nothing in the CA or technical framework at this stage for patient matching. We support efforts to discuss the current policies, practical objectives, potentially unnecessary or restrictive barriers (e.g., notarized documentation requirements), and available technological solutions for patient matching within the industry as a priority, and we encourage more public forums to discuss this area since no industry agreed-upon standard exists.

Identity Proofing is also not addressed in the CA, and an intent to develop a SOP was discussed. Properly identifying individuals and ensuring accurate identities in information exchange to evidence that individuals are, in fact, who they claim to be are critical to promoting confidence and trust in the system.[2] Existing HHS/OCR regulations and guidance can help frame the work ahead while the RCE and stakeholders further clarify these parameters for the TEFCA roles and needs.

- **Non-TECFA Entities.** We recognize that at this stage participation is voluntary, and no individual or entity is required to participate. Some entities may want evidence of proven results and a track record of performance before engaging in these processes. Until evidence-based results are achieved, the RCE, working with ONC and other federal entities, should clarify how no private individual or entity will be disadvantaged in the marketplace for waiting or for deciding not to participate in the TEFCA infrastructure. In other words, while the goal will be to achieve interoperability, efforts should be made to ensure that no significant disparate impacts result for non-participating persons or entities who still need to be part of the health care ecosystem supplying and accessing complex and diverse services, until such time as they have confidence in this new and unproven system and have built sufficient IT and compliance infrastructure to meaningfully participate.

If you have any questions, feel free to reach out to me at dlloyd@ahip.org or 202-778-3246. We look forward to working with you in support of this laudable goal of achieving seamless data exchange across the healthcare ecosystem in a manner that reduces administrative burden and infrastructure costs at the same time it improves patient outcomes and access to affordable care.

Sincerely,

Danielle A. Lloyd

Danielle A. Lloyd
Senior Vice President, Private Market Innovations and & Quality Initiatives

AHIP Proposed Elements of the Common Agreement

Attachment A

Exchange Purposes

Transactions

In the initial stages, QHINs will be expected to support:

- Treatment
- Payment
- Health Care Operations
- Public Health
- Benefits Determination
- Individual Access Services

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 eligible for such transactions.

Response: We generally support the purposes of these initial functions and agree that they can serve as a starting point from which to add future services and connectivity. The CA Elements note that treatment, payment, and healthcare operations (TPO) will generally have "the same meaning as they do under the HIPAA privacy rule," and apply to all TEFCA information regardless of parties' status or relationship. We support this concept and believe it is the correct approach.

There are a few significant issues that we believe should be clarified before final terms are developed:

- For QHIN-to-QHIN exchanges, it is unclear whether it is appropriate to limit a request to only one purpose or if implementing such an approach could become inefficient and problematic.
- Uses and disclosures are to adhere to the CA privacy and security requirements "and any applicable privacy notices." We believe this should also specify "applicable laws and regulations" (as discussed above).

- Uses and disclosures should adhere to the CA privacy and security requirements and "flow down" provisions. At present, it may appear that only some of the CA provisions will flow to Participants and Sub-participants and stakeholders need to better understand what provisions apply, when, and to which entities.
- More details are needed to fully evaluate the specific "required" and "permitted" responses. For example, it is unclear when or whether individual consent will be required to share information (e.g., to a public health authority, to a non-health public agency).
- Only the six exchange purposes will be included at this time but no other important functions (e.g., biomedical research which may be added in future installments). For planning, anticipated exchange purposes beyond the initial six listed could be inventoried, and a working list and timetable be developed for building them into future versions and upgrades.
- We request that your organization work with stakeholders to explain TPO, such as through use cases of data expected for QHIN-to-QHIN exchange. Since some entities will be unfamiliar with these terms in relationship to HIPAA and their practical applications; education in this area will be helpful.
- We appreciate the inclusion of benefits determination data. We ask that the final draft, as well as future iterations, continue incorporating appliable laws and updates, including consumer awareness and opt-out options regarding the sharing or use of this information.
- We value the incorporation of public health data. During the pandemic, the inability of stakeholders like health insurance providers to access information such as vaccination status greatly hampered broad contributions to public health goals. Going forward, we will look for ways to support electronic linkages as part of TEFCA and other processes.
- The exchange purposes currently described in the CA are for "Request-Response" between stakeholders. Inclusion of additional approaches (e.g., a publish-subscribe model) may allow real-time dynamic information updates across all authorized participants without the need for pushing the requests and pulling the responses, and this functionality could promote better functionality for care coordination and chronic condition management.
- We support the inclusion of social determinants of health (SDOH) data into TEFCA and the CA over time. We request that SDOH data be considered for inclusion and exchange as data standards such as ICD-10, USCDI, and the Gravity Project become mature or are updated. Creating the ability for stakeholders to

easily exchange these data will enable a better understanding of the impact of SDOH, identify interventions that mitigate SDOH, and improve outcomes.
- We ask the RCE to leverage a stakeholder consensus building effort when determining future use cases for exchange.

Connectivity

TEFCA requests would be transmitted via a QHIN's Connectivity Services and will be consistent with the requirements of the Qualified Technical Framework (QTF), including when queries are made for health information. QHINs, Participants and Sub-participants that receive requests for data on an individual, and that hold such data, will be required to respond with the data (unless an exception applies). Responses will be permitted but not required for specific situations, such as a Public Health Authority, a governmental agency (including its agents or contractors) that determines non-health care benefits, and other situations.

Response: We fully support uses and disclosures following the HIPAA privacy and security requirements and covering non-HIPAA entities through contracts. For QHIN-to-QHIN exchanges, "Treatment," "Payment," and "Health Care Operations" will have the same meaning as under the HIPAA Privacy Rule and would apply to all TEFCA Information, regardless of whether or not the parties to exchange are HIPAA Covered Entities or Business Associates. That approach is sensible and should help ensure consistency across platforms and entities.

We are concerned about specific processes that require a data release unless an exception applies. In an electronic environment, required responses facilitate ease of operations and reduce costs. Exceptions, however, have a converse effect and complicate workflows and increase costs, often without a substantial benefit to an individual. We would need more information about the use cases for exceptions to more-fully evaluate the expected costs, benefits, burdens, and workflows. At present, it is unclear how an entity can determine an exception applies, particularly when thousands or more transactions are expected once the infrastructure is up-and-running. We believe that several issues need to be explained for entities to become involved in the TEFCA processes. For example, we recommend more clarification for oversight, possible auditing, and enforcement.

- Will these functions generally be left to the contracting parties?

- Will audits be required either by the RCE or the Participant and Sub-participant agreements? If so, who bears the costs?
- Does the RCE expect to become involved in oversight, auditing or enforcement, and if so, under what circumstances?
- What, if any, role will ONC have in these processes?

These variables can impact whether entities want to voluntarily be part of the TEFCA processes and would benefit from further explanation.

Participants and Sub-participants

The CA would enable a network of networks of high-performing, reliable, and secure QHINs to share health information. Each of the QHINs would support exchange on behalf of the respective Participants with which they have a separate data sharing agreement. In turn, Participants could enter into information sharing agreements with one or more Sub-participants. This "network of networks" would have at least three layers consisting of QHINs, Participants, and Sub-participants (e.g., a physician practice, hospital, pharmacy, or public health agency). Stakeholders would connect at the point that is most appropriate for them (e.g., a health information exchange, health IT software developer, health care system, payer, or federal agency could each be a Participant).

Response: We support the current proposals and look forward to learning more about which entities can fit into each of these categories. One of the challenges confronting organizations operationalizing the requirements of the CMS Interoperability and Patient Access final rule and ONC Cures Act final rule is that there can be a lack of trust between the parties required to exchange data. Normally a governing legal contract is in place, but under these rules payers and providers have to share information with any entity the consumer designates, with few exceptions. The CA could be an avenue to foster trust between payers, providers, and other stakeholders. Moreover, it could create efficiencies if, for example, third party developers connected through TEFCA creating a single registration and agreement point.

At present, it can be difficult to envision which entities will fall into which category, particularly as companies and information systems have become so increasingly complex and an entity's legal status can vary based on the function performed (e.g., a health insurance company may fully-insure benefits or it may act under an

administrative-services only contract delivering services to an employer group that is fully insured). Corporate relationships (e.g., HIPAA business associate, non-HIPAA vendor) may be connecting into the system and depending on their function and purpose it could be hypothetically possible to be classified in one or more categories based on what function they plan to perform. For example, a QHIN may have concerns with a Participant or downstream Sub-participants, or a Participant may be uncertain about a QHIN or Sub-participant. More information about entities, roles as they relate to these definitions and functions, and the applicable "flow down" provisions are needed.

We are unsure about the ability for QHINs and Participants to enable Sub-participants. More understanding is needed for the vision of how this will roll-out, especially if QHINs are not aware of new Participants and Sub-participants and whether they are or are not HIPAA-covered entities. We encourage Sequoia to continue discussions across stakeholders.

Required "Flow Down" Provisions

The CA sets out certain provisions that QHINs would be required to include in their Framework Agreements with Participants and that Participants would be expected to include in their agreements with any Sub-participants (called "Required Flow-Down" provisions). The required flow-down provisions would address:

- cooperation and nondiscrimination;
- confidentiality;
- utilization of the RCE Directory Service;
- uses, disclosures, and responses;
- Individual Access Services (IAS);
- privacy;
- security; and
- other general obligations.

Response: We look forward to learning more specifics about the flow-down requirements and what will happen if a contractual breach occurs. The CA and "Flow-Down" provisions do not replace HIPAA but would extend many of the HIPAA Rules to entities that are not HIPAA entities. Understanding the compliance expectations and enforcement of violations is needed.

We recommend the next iteration of the CA and related contracts add performance, scalability, and reliability elements as requirements. We also recommend the CA flow-down provisions include guidance for handling Federal and State contracts as well as employee groups.

TEFCA Information and Required Information

TEFCA Information is any information that is exchanged between QHINs for one or more of the Exchange Purposes. Most of the QHINs, Participants, and Sub-participants will be subject to the HIPAA Rules, so much of the exchanged TEFCA Information is expected to be HIPAA electronic Protected Health Information (ePHI). TEFCA Information can include HIPAA de-identified information. A QHIN, Participant, or Sub-participant that receives a request would be obligated to provide all Required Information for the Exchange Purpose, unless prohibited by applicable law or one of the Framework Agreements.

Response: We are concerned about the breath and scope of this provision; it appears overbroad. Under the HIPAA privacy regulations, once information is de-identified it is no longer considered PHI. In addition, TEFCA Information would not be limited to health information and presumably information about topics not related to health (e.g., environmental health information sent to a public health organization, or information not related to an individual) will be exchanged via QHINs and become subject to these requirements. Including de-identified and other non-PHI categories of information appears to conflict with HIPAA's parameters. The RCE should not include de-identified data in these definitions and processes.

Governing Approach to Exchange Activities Under the Common Agreement

The CA will specify the way in which QHINs, Participants, and Sub-participants may participate in oversight of activities, how the CA may change, and resolution of disputes. The governing bodies will serve as a resource to the RCE and provide a forum for discussion of CA exchange activities. The CA will create an Interim Transitional Council for a 12-month period, followed by the permanent Governing Council. The QHIN Caucus and Participant/Sub-participant Caucus will elect members to the Governing Council. ONC will oversee the work of the RCE and ONC approval is required for amendments to the Common Agreement, the SOPs, and the QTF.

Response: The governance approach is somewhat complex – a series of Governing Bodies which will serve as a "resource" to the RCE and a series of Advisory Groups that could be established "as needed." Given that the needs criteria are not yet known nor is the entity or individuals who can decide that a need requires action and advice, a complete Governance Framework could be a different but better approach, with definitions and details for who, what, when, where of the bodies that will 'govern' TEFCA.

The process for filing and resolving disputes remains unknown. We request that these be spelled-out in the CA.

QHIN Designation and Eligibility Criteria

Only the RCE will be able to designate a QHIN under the CA. The RCE is establishing an application and assessment process to designate QHINs based on eligibility criteria, including: (1) the ability to perform all of the required functions of a QHIN, as identified in the QTF; (2) the legal structure and governing approach for the QHIN; and (3) demonstrated resources and infrastructure necessary to support a reliable and trusted network. Some entities can be allowed to join on a provisional 12-month basis, subject to additional scrutiny and monitoring.

Response: We recognize the intent of these criteria is to build a reliable "backbone" that will support a functioning exchange. We question, however, whether some entities may be unfairly "shut out" and unable to participate, potentially leading to unfairness and undesirable concentration of QHINs.

We believe that RCE would benefit from considering expert and other advice on this issue. Therefore, rather than offering a specific recommendation, we encourage the RCE to consult with start-up organizations, smaller entities, small business owners and antitrust experts who can help RCE appropriately address potential concerns in this area.

We note that the12-month provisional access may also inhibit new exchange solutions and reduce innovation and competition. We recommend reducing or reconsidering the provisional period as a means to balance opportunities between new and existing exchanges and in order to avoid inappropriately discouraging or preventing the beneficial impacts that new entrants can bring.

The 12-month provisional status includes additional reporting and monitoring. We seek additional details on the reporting and monitoring structure.

We also request additional clarification on the following:

- How will authentication be handled by the QHINs, Participants and Sub-participants?
- Will a security or "audit trail" be required?
- How is provenance considered?
- Who will have the capability to conduct audits and to whom should records be made available if requested?
- Currently, health information exchange participants know about other HIE participants. Under the CA, will a mechanism exist for HIEs to add Sub-participants without QHINs, Participants and others knowledge?

Cooperation and Nondiscrimination

The CA would specify expectations of QHINs, Participants, and Sub-participants that would ensure that all parties cooperate in certain aspects of exchange such as timely responses to inquiries, notification of persistent and widespread connectivity failures, support in resolving issues, and sharing information regarding cybersecurity risks. QHINs, Participants, and Sub-participants would be prohibited from limiting interoperability with any other QHIN, Participant, Sub-participant, or Individual in a discriminatory manner.

Response: AHIP is an active participant in the Heath / Public Health Sector Coordinating Council and we serve on the Executive Committee for Cybersecurity. AHIP, working with our public and private partners, has long-standing experience in promoting effective cybersecurity practices. We promote information sharing to help identify, detect, combat and respond to many cybersecurity events. We have helped develop and collaborate on a wide-range of substantive guidance and educational documents.

Our experiences have shown that information sharing across entities is critical to cybersecurity. Particularly in the healthcare system, one cyber-attack can take down critical and essential, health care functions. Entities need the ability to share timely

information to help each other maintain the security and operations of U.S. healthcare systems.

The CA could benefit from more detail about the expectations for information sharing, particularly for cybersecurity preparedness, risks, threats, vulnerabilities, attacks, etc., as well as how to handle and report data breaches between parties within and between QHINs (or by QHINs themselves) and Participants and Sub-participants. We encourage the RCE to develop detailed CA and other contractual provisions for identifying, investigating and reporting data breaches. This should include specifics for reporting to federal and/or state regulatory bodies as required by law or regulation. In addition, we recommend additional details explaining: (1) the network participants and connectivity points; (2) required "downtime" for making updates; (3) responding to cyber, data breach events, and other extenuating circumstances that can affect the overall operations; (4) the communication protocols across participants in these scenarios; and (5) issue resolution and expectations (e.g., "all clear" operations, 24/7 support, response times).

RCE Directory Service

The RCE will maintain a Directory Service to support exchange of information between and among QHINs, Participants, and Sub-participants. The CA will identify the rights and limits on use of the RCE Directory Service (e.g., the directory information will be prohibited from being used for marketing purposes). The RCE will investigate misuses of the directory (e.g., "poaching" customers).

Response: A directory service will enable greater data sharing as it reduces the overhead of each entity developing this service. In this section, we respectfully request the following clarifications:

- What is going to be in the Directory Service?
- Where is the data coming from and to where will it be going?
- How will the directory be maintained?
- Who/what entities will have access to it?
- Will existing digital end-point directories be utilized and will other vendor solutions integrate? What are the permitted purposes of use?
- What are the prohibited purposes of use?
- What are the consequences of prohibited uses?

- How will updates and corrections be made and by whom?
- Whether and to what extent will the service rely on patient or provider matching?
- How or will the service support access, communications, and exchanges?
- Will there be a cost for the maintaining, using, and/or accessing the Directory Service?

Individual Access Services (IAS)

IAS Overview

IAS would be the services any QHIN, Participant, or Sub-participant provide to an Individual to satisfy that Individual's request to access, inspect, or obtain a copy of that Individual's TEFCA Information that is maintained by any QHIN, Participant, or Sub-participant. A QHIN, Participant, or Sub-participant would be allowed, but not required, to offer IAS to Individuals with whom they have a Direct Relationship. The CA anticipates the use of consumer-facing applications that would assist Individuals in obtaining access to their health information.

Each QHIN, Participant, and Sub-participant that elects to offer IAS to Individuals would be an IAS Provider. IAS Providers would be allowed to make requests on behalf of Individuals for data from all other QHINs, Participants, or Sub-participants using the IAS Exchange Purpose. QHINs, Participants, and Sub-participants that receive such requests and hold that Individual's Required Information would then be obligated to respond with that data, unless an exception applies.

Response: We understood that the IAS would be a primary function of the TEFCA processes or may be planned for later stages. We recommend that this section be clarified and, in the future, it either be required within a specified time (e.g., one year following a signed contract) or listed as a priority for future implementation stages.

A layered approach to IAS is highly recommended and could start with consent and be limited to consent or revocation of data being shared as a "first layer." As the authentication and verification model is more fully developed, then additional data access could be added. This would ensure that privacy and security concerns have been fully analyzed and addressed. (We discuss consent more broadly in the specific Consent section below.)

We request further stakeholder discussions and buildout of the technical framework to ensure full and secure function.

We also request clarification of the following questions:

- What will be the preferred authentication model for individual access and will more than one approach be used?
- Of what will the consent management process consist?
- How would the technical framework work in this context?

Privacy Notices and Individual Rights

The CA's IAS requirements will specify the elements of a written privacy notice to include a description of the need to obtain express consent from Individuals regarding the way their information will be accessed, exchanged, used, or disclosed. IAS Providers would need to implement security measures. The CA will also specify Individual rights that IAS Providers would need to provide, such as:

- the right to have deleted all of their individually-identifiable information maintained by an IAS Provider.
- the right to obtain an export of their data in a computable format.
- the requirement to obtain express written individual consent to sell individual data.

Response: AHIP has long-supported prohibitions on the sale of individually identifiable without consent. We support maintaining this prohibition in future drafts. It is unclear whether a prohibition on sale of data could apply to de-identified data sets, particularly since the existing HIPAA regulations for de-identification did not anticipate interoperability at the time they were enacted. The RCE should consult with OCR to further evaluate potential implications and unintended results.

It is uncertain whether the requirement to delete an individual's data can realistically be achieved, particularly once disclosures are made. Specific parameters are needed if entities will be expected to comply with this expectation. We strongly caution against finalizing this right at this stage to avoid patient safety issues and negative health outcomes. Perhaps it could be implemented at a future time, and after additional stakeholder input, but not at this stage.

It is also unclear whether the CA will specify additional privacy and security requirements to which a QHIN, Participant and Sub-participant will be required to adhere or whether these requirements will be the existing HIPAA rules. We would not recommend setting up duplicate or conflicting rules in these processes that could make IAS more difficult without achieving a substantial benefit to individuals. That being said, for sale of individually-identifiable data, we remain concerned with the degree to which third party apps will be able to access data under the "IAS" purpose yet remain outside of the strict privacy and security controls and requirements of HIPAA (and thus create an unequal field for covered entities and business associates). While the intent to bring the apps into a HIPAA-similar structure is the goal, in reality, legal enforcement processes are lacking without future Congressional and regulatory action.

The specific elements to include in a privacy notice have yet to be announced. We encourage this effort to streamline future requirements with existing notices to avoid substantial cost and re-writing/re-issuing of Privacy Notices. We support making these notices available electronically, in lieu of a printed document, unless a printed version is requested by an individual.

In addition, one of the webinars clarified that stand-alone notices will not be required and privacy notices could meet the TEFCA and other purposes simultaneously. We encourage your organization to make this clear in future CA versions or SOPs.

Privacy and Security

The CA will promote strong privacy and security protections and promote trust. Most entities will be HIPAA Covered Entities or Business Associates and comply with the HIPAA Privacy, Security, and Breach Notification Rules. For non-HIPAA entities, the CA would require protection of individually identifiable TEFCA Information in mostly the same way as HIPAA.

QHINs would be expected to meet and maintain third-party certification to an industry-recognized cybersecurity framework and to undergo annual security assessments. The CA will specify security incident notifications affecting QHIN-to-QHIN exchange applicable to QHINs and the "flow down" Participants and Sub-participants. The RCE will facilitate information security.

Response: We strongly support the expectation that Participants and Sub-participants that are not subject to HIPAA will be required to comply with substantially the same requirements, although we remain concerned that some entities or apps will be able to continue to operate outside of the realm of HIPAA in practice. In other words, because the statutory and regulatory requirements do not cover these entities, and they will be bound by contractual expectations, situations could arise where a technical HIPAA violation occurs (if it were committed by a covered entity or a business associate), but the non-HIPAA entity garners no real consequences for non-HIPAA compliant actions. While our concern may be hypothetical at this juncture, we seek feedback from the RCE as to how these potential scenarios could be avoided.

We support leveraging existing, national security certifications such as using the National Institute of Standards and Technology cybersecurity framework or the HITRUST Common Security Framework to meet the third-party certification. This will avoid the need for duplicative processes and increased, unnecessary costs.

For individually-identifiable information, we note prior regulatory developments that should be considered in the TEFCA context. We await final federal regulations from HHS/OCR explaining the HIPAA Privacy Rule and allowing social service and similar organizations to receive individuals' health information for care coordination purposes. The regulations may clarify the scope of covered entities' abilities to disclose PHI to social services agencies, community-based organizations, home and community-based service (HCBS) providers, and other similar third parties that provide health-related services that may or may not be a health care provider (e.g., food or sheltered housing needed to address health risks). A newly proposed subsection would expressly permit disclose of PHI to such organizations that provide health-related services to specific individuals for individual-level care coordination and case management, either as a treatment activity of a covered health care provider or as a health care operations activity of a covered health care provider or health plan. If these disclosures will be made to business associates engaged by a CE, (e.g., a health plan's BA provides health-related services to an individual), then the CE must have a HIPAA-compliant Business Associate Agreement (BAA) in place prior to disclosing the PHI. In other cases, the entity receiving the PHI will be providing health-related services on its own behalf, and not performing covered activities or functions for or on behalf of the disclosing CE, so a Business Associate Agreement will not be required. In addition, some of the third-party recipients of PHI may be health care providers or covered health

care providers under HIPAA which can perform care coordination and case management for their own treatment activities or health care operations. In general, we supported the intent of the regulatory proposals for improving care coordination and meeting the social, physical and psycho-social needs of individuals improve overall well-being and health outcomes. We cautioned HHS/OCR about the lack of vetting processes for community-based organizations. Not all organizations effectively serve the individuals they purport to represent. We expressed reservations about extending this flexibility too broadly. We also highlighted the sensitivity of PHI data surrounding issues such as substance use disorder and HIV status. We encourage the RCE to model TEFCA requirements to conform with final HIPAA regulations, if promulgated.

Special Requirements (including Consent)

Uses and disclosures of TEFCA Information will be subject to HIPAA and other applicable federal and state laws. The CA will not require QHINs, Participants, and Sub-participants that are not IAS Providers to obtain individual consent to use or disclose TEFCA Information, unless they are required to do so under applicable law. The CA will require IAS Providers to obtain express consent from individuals for how information may be accessed, exchanged, used, or disclosed, including whether that information may be sold.

Response: We support the proposed approach for not requiring individual consent for uses and disclosure of TEFCA information, apart from IAS. The CA appears to establish, however, a new level of consent for IAS providers that broadly covers express consent for access, exchanges, uses, and/or disclosures. This appears to be an expansion of consent, particularly if the purpose of the IAS is to provide access services to the individuals that are subject to the information. In other words, broad express consent from the individual would be required from the individual to allow him or her to access their own data. In situations where consent documents may be shared, the QTF has proposed a mechanism for QHINs, Participants, Sub-participants, and individuals to share such electronic documents with each other.

We agree that the CA should not conflict with or affect state laws that require consent for different purposes, including treatment. The HIPAA Privacy Rule permits, but does not require, a covered entity to obtain consent for uses and disclosures of PHI

for TPO. Likewise, we agree that the CA should not create a national opt-in or opt-out registry as HIPAA does not have such requirements.

Specifically regarding technical specifications, there are questions relating to using "line item" consent on categories of sensitive information as could be evidenced on a HIPAA authorization form. Each participant could have their own interpretation of what constitutes sensitive codes based on their interpretation of the privacy laws applicable to their state and local regulations. As discussed above, entities need to understand how to handle these situations if a national infrastructure will be workable. We recommend that ongoing education explain how consent requirements are different from the HIPAA written authorization and related processes. It would be advisable to explain whether a written HIPAA authorization can constitute consent requirements in the TEFCA environment.

The CA does not explain if or how consent may be forwarded. For example, if two payers have both signed the CA, it is unclear whether one payer can forward a consent (excluding sensitive conditions) to a prior payer to allow data to flow from a previous payer through automation.

While technical parameters have been discussed, many issues remain ranging from:

- sufficiency of what constitutes "consent;"
- how it can be obtained (e.g., variation across entities, whether forms can satisfy the requirement, will this be a "click through procedure, etc.);
- how revocations will be handled;
- how consent will be transmitted and "carried forward" to other entities in the exchange, and many additional factors.

We seek answers to the following questions:

- Is consent management being considered as a part of the disclosure process?
- How or will existing CMS mandates and contractual expectations intersect with TEFCA?
- How will individual consumers be authenticated?
- Will rules be set for a fair exchange of data?
- Who will be accountable for data quality?

- Are non-HIPAA entities able to participate and submit requests for exchange purposes?
- How will HIPAA authorizations and consent forms be stored and shared between QHINs?
- For how long with HIPAA authorizations and consent forms be maintained and deemed valid in the TEFCA environment?
- What will the revocation process be and how will changes to authorization or consent forms be communicated to the entities?

Fees

A QHIN will be unable to charge fees to other QHINs with respect to activities under the Common Agreement. QHINs would not be prohibited from charging fees to Participants.

Response: As a primary matter, we believe the impact to individuals should be explained. It is currently unclear whether individuals will directly or indirectly incur fees, which could prohibit access to their own information. We expect that this is not an intended result and would appreciate clarification for individuals.

We are also concerned about the possibility of "nickel-and-diming" entities and/or individuals through per-transaction, per-time usage, or similar fees, rather than an expected, flat fee for all exchanges. Years ago, clearinghouses and trading partners using the HIPAA electronic transactions and code sets grappled with similar issues and not all parties were satisfied with the end results. The CA should also clarify any specific structures, fee or data caps, or other limits.

Additionally, CA fees could apply in addition to other existing fees charged by certain entities (e.g., HIEs if Participants or Sub-participants). It is unknown the effect, if any, these provisions may have on existing contracts and payment arrangements. We recommend consulting HIEs to further understand the existing, future and sustainable fee structures and existing contracts.

We do not yet know who will be QHINs or what their pricing structure will be. Some may offer services more than the base minimum requirements in the CA (e.g., a research component). In prior discussions, it was deemed amendable for entities to charge for

above-the-minimum services. That information should be explained in future CA versions.

We recommend starting with the purposes of the fees and determining the minimum fees necessary to support appropriate purposes. Fees should always be limited to the minimum necessary to accomplish necessary purposes. Next, we recommend that you consider the ways that such fees can create a barrier to participation and take steps to ensure that fees do not have this impact. We also recommend further public dialog before making a final determination on fee levels and fee structures. It is important that any fees do not limit competition or undermine the benefits contemplated.

Definitions

The current CA definitions do not define "indemnification."

Response: A definition of indemnification should be added, if it will be required as part of the CA or any of the flow-down or other contracts.

Other Issues

- **Blockchain and Other Technical Solutions.** The QTF and the CA should consider additional interoperability update needs and enable the use of advanced solutions like blockchain-based technologies as an option for QHINs, Participants, and Sub-participants. Likewise, the RCE should support blockchain and distributed ledger technology (DLT) as a means of architecture. The next version of the CA, the QTF, or future SOPs should address standards around how a blockchain-based QHIN would communicate to a non-DLT QHIN.

  These technology solutions offer assured privacy and security support. Future privacy and security provisions should consider how blockchain arrangements can be leveraged (e.g., to solidify via code who has access to the different data or "proof of data" along the chain). Furthermore, combining blockchain and APIs, PHI can be stored off the chain, creating greater protections of privacy and security. Blockchain technologies can offer traceability and details of what is accessed, by whom, and when and the distributed nature of the network significantly reduces the likelihood of data breaches or attacks. In support of these exchange purposes and tracking, we

request the RCE ensure the ability of blockchain and distributed ledger technologies be leveraged by QHINs, Participants, and Sub-participants.

- **Contingency plans.** Despite best efforts, new processes and functions do not always transpire without effort and error. We would like to learn more about the plans that will be implemented if initial roll-outs do not function as intended.

  We also request guidance on how to engage with other payers that choose not to enter into the CA. If one payer refuses to support the CA and another payer does support the CA, what could be the expected impacts?

- **Future Gazing.** A preliminary roadmap for future plans can be helpful, even in draft form, to offer specifications, including: (1) new exchange purposes, such as whether Explanation of Benefits will be included; (2) new data to be stored and exchanged and when and how cloud functionality can be utilized; (3) in case Participants or Sub-participants access or use "off-shore" entities or business functions, whether these can be allowed or will be blocked; (4) for how many years' will data be stored; (5) what governance changes may be expected; (6) general expectations for record retention; and (6) how data release agreements and related documentation will be handled within the framework.

QHIN Eligibility Requirements

We will continue to evaluate the proposed QHIN eligibility requirements, which include 5 general criteria:

1. It must be a U.S. Entity.
2. Is able to exchange required information as defined in the CA.
3. Is able to demonstrate that it has the ability to perform all of the required functions of a QHIN.
4. Has the organizational infrastructure and legal authority to comply with the CA.
5. Has the functional and technical ability to comply with the QHIN Technical Framework.

On the RCE's October 14, 2021 webinar (and as available by recording) there was specific discussion of allowing foreign entities as part of the process. As described during the event, an entity could technically be a U.S. entity but could have foreign

ownership (and perhaps foreign funding). The RCE speaker noted that future guidance was being developed on this topic.

The present concern appears to be that cybersecurity and other vulnerabilities could arise. However, we believe this is a much broader issue, as nation states have sponsored cyber-attacks in some contexts, and in other situations, could foreseeably access individually-identifiable and/or private and public confidential and proprietary data. These are vulnerabilities that merit serious consideration before foreign entities are allowed in this U.S. process.

There is also concern that patient data could be "offshored" in some capacity if a foreign owner or funding source is ultimately in charge of the corporate entity. This is a realistic concern, particularly when governmental regimes significantly control or own “private” companies operating in those countries. Many federal and state health benefits contractors must adhere to specific data security rules that prohibit offshoring on individuals’ health data. These requirements should be considered and the potential impact on U.S. consumers before any allowance is made to include foreign entities in the TEFCA processes.

As discussed above, we are concerned that the potential 12-month provisional QHIN status may inhibit new exchange solutions and reduce innovation and competition. We recommend reduction of the provisional period as a means to balance opportunities between new and existing exchanges.