Trust Exchange Framework and Common Agreement Public Comment Summary

Contents

General

- **General Reaction**: Respondents general reaction to the Trusted Exchange Framework and Common Agreement (TEFCA) fall into three rough camps:
    1. **Supportive**: These respondents generally think ONC should push hard to address variability in network-to-network exchange that is inhibiting the flow of data today. While supportive of existing efforts these respondents were generally less concerned about the potential to disrupt existing activities.
    2. **Cautiously Supportive**: These respondents generally think ONC should do more to address variability in network-to-network exchange but expressed strong concerns that the output of the TEFCA, whether intentional or not, could disrupt existing exchange efforts. These respondents generally felt existing efforts were making good progress but more coordination and alignment across them was required.
    3. **Very Concerned:** These respondents expressed strong concern about ONC's potential direction with the TEFCA and encouraged ONC to focus on developing general principles through guidance to address gaps in existing frameworks and promote alignment across the industry. They feel, while additional progress is needed, that the industry is headed in the right direction and that major changes would slow rather than accelerate progress. They stressed ONC should not establish specific requirements that existing networks must follow or create a new entity to replace the work of existing organizations. These respondents felt any effort to implement an approach to the TEFCA that mandates change in existing trust arrangements will meaningfully disrupt current exchange efforts and impose significant costs on all participants by requiring changes to existing networks, BAs, and other agreements. Any change that require modifications to the arrangements' agreements will require them to be renegotiated and resigned by all participants and their end users.
- **Avoid Disrupting Existing Efforts**: Many respondents noted that ONC should ensure it avoids disrupting or duplicating the work of existing networks that are in operation today and successfully enabling data exchange. Many also recommended that the approach to the TEFCA should be truly voluntary in nature with a high degree of transparency regarding participation.
- **Recommended Principles for the TEFCA**: Respondents recommended a number of principles that ONC should consider in establishing the TEFCA
    - Build off the existing foundation of interoperability solutions and existing networks with a focus on enabling network-to-network exchange by only addressing areas that require standardization and alignment to enable existing, and potentially new, networks to exchange across one another.
        - Certain variance across networks can remain and are reasonable. ONC's focus should be on areas that must be standardized to enable cross network exchange.
    - There is no one size fits all solution to interoperability, the TEFCA should not try and establish a single approach to address all data exchange needs.
    - The TEFCA should be flexible enough to reflect and accept network-based differences in implementations and local and state policy differences.
    - ONC should pursue an approach that reduces the cost and technical barriers to support the ability of small providers and health IT developers to participate.
    - The TEFCA should establish a floor not a ceiling for data exchange.

  - Ensure the approach is adaptable and implementable by a variety of organizations that have differing business models, technical approaches, and capacities.
  - Ensure there is an enforcement mechanism that can and will be applied if a participant fails to meet the TEFCA requirements.
  - Avoid unnecessarily limiting innovation or variation.
- **Recommended Components of the TEFCA**: Respondents recommended a variety of components that should be included in the TEFCA. In addition to the six categories that ONC outlined the following were mentioned:
  - Permitted purposes of data use (aligning data uses with HIPAA was a common theme)
  - Breach notification (including standardizing the reporting requirements)
  - Liability limitations
  - Accountability mechanisms such as independent accreditation
  - Standardized use cases
  - Link the data blocking provisions of 21st Century Cures to the TEFCA
  - Enforcement mechanism
  - Dispute resolution process
  - Data quality requirements
  - Patient matching standards
  - Approach to addressing varying authorization policies
- **Recommended Use Cases**: As noted above, respondents requested ONC include standardized use cases in the TEFCA. Respondents also requested ONC prioritize among use cases and provide clear implementation timelines. A number of potential exchange use cases were mentioned including:
  - Provider-to-provider
  - Provider-to-consumer
  - Care coordination
  - Closing the referral loop
  - Query/response
  - Push (including automated pushes)
  - Consumer access
  - Consumer mediated exchange
- **Clear Definitions of Terms**: Some respondents requested ONC establish clear definitions of a health information network and trusted exchange framework, including what the qualifications for becoming a trusted exchange framework are and what types of entities do and do not fit under the definitions.
- **Consumer Access**: Many respondents felt the TEFCA should include components to address providing patients' access to their health data. Some respondents felt ONC and OCR should provide guidance to the national trust arrangements to promote their adoption of patient access use cases.
- **Other**:
  - **Guidance on Incorporating and Retaining Data**: A few respondents noted that health IT developers and providers are in the early stages of figuring out how best to utilize the data they receive via HIE and encouraged ONC to support efforts to improve these processes and develop best practices. One respondent noted that it would be helpful to have greater regulatory clarify on record retention requirements for data received via HIE (what data must be retained, for how long etc.).

- **Onboarding Path for TEFCA**: A respondent recommended ONC include a simple testing path for potential participants who want to try out the TEFCA that includes piloting opportunities and the ability to terminate participation within a defined time period (i.e. 90 days).
- **Applicability**: A few respondents noted that it is important for the TEFCA to cover the full range of participants in HIE and not just cover one actor (i.e. EHR developers).

Standardization

- **General Reaction**: Respondents agree that standardization is an important component of the TEFCA.
    - Many respondents noted the importance of continuing to leverage existing standards and implementation specifications that are the foundation of the current state of interoperability. Significant investments of time and dollars have been put into existing interoperability approaches by health IT developers, providers, networks, and trust arrangements, starting from scratch would be a waste of the these prior investments.
    - Some respondents recommended an aggressive government lead push to expand the set of standards and implementation specifications required, while others recommended a reduced role for the government in furthering the adoption of standards.
    - Some respondents recommended that ONC not require a specific technical or organizational architecture in the TEFCA, noting that that centralized and federated models can work together.
- **Recommended Standards Categories**: Respondents identified a variety of categories of standards and implementation specifications that are important to enabling interoperability including:
    - Transport
    - Content
    - Vocabulary
    - Security
    - Semantic
- **Use Cases**: Standards and implementation specifications included in the TEFCA should be clearly linked to specific use cases whose prioritization/selection should include providers and health IT developers.
- **Alignment with ISA**: Respondents requested that ONC ensure alignment between any standards outlined in the TEFCA and those included in the ISA.
- **Patient Matching**: Many respondents suggested patient matching between networks should be addressed as a components of the TEFCA.
- **Other**:
    - **C-CDA Improvements**: Some respondents requested ONC expand the core set of required data elements in a C-CDA and work with the industry to develop guidance on uniform look back periods for contents of the care summary documents (i.e. 3 months, six months, one year etc.).
    - **Identity Proofing**: The TEFCA needs to include strong identity proofing requirements for patients and providers. A number of respondents felt ONC should leverage existing NIST requirements when establishing these requirements.

Transparency

- **General Reaction**: Respondents were generally supportive of this principle. Some respondents were unclear on what the principle referred to though and expressed that they strongly supported the principle in the context of transparency in the terms and requirements of trust arrangements.
    - Respondents generally felt it was important to establish a common approach to transparency across networks. Some also noted the importance of defining the boundaries of where the transparency requirements apply and what limitations are allowed to protect the privacy and security of PHI.
    - Some respondents encouraged ONC to develop core principles that would apply to all trust arrangements to enable essential consistency across networks but avoid attempting to draft detailed service level or network agreements.
- **Recommended Transparency Requirements**: Respondents suggested a number of transparency requirements that should apply including publically posting:
    - Data sharing agreement(s)
    - Use cases
    - Standards/implementation guides
    - Participants
    - Exchange metrics
- **Data Blocking**: Some respondents noted that data exchange today happens through a variety of mechanisms and standards that all that provide value to providers, patients, and other end users leveraging the mechanism. These respondents encouraged ONC to ensure organizations that choose to use methods of exchange other than those covered in the TEFCA not be considered de facto information blockers.
    - Some respondents encouraged ONC to identify configurations or workflows that unnecessarily limit exchange but fall short of information blocking.
- **Governance Requirements**: A few respondents noted the important of ensuring baseline requirement for the governance approach and makeup of the governing board of participating health information networks/trusted exchange networks.
- **Local Policy Flexibility**: A few respondents requested clarification on if the TEFCA would provide flexibility for local decisions to be made about who to trust or if it will require participants to openly and transparently exchange with all parties of the TEFCA including those that they would not otherwise choose to trust.
- **Transparency of Data Exchange to Patients**: A few respondents asked how patients fit into the transparency requirements. Some requested greater patient control over how their data is exchanged while others requested great transparency in how their data is exchanged.
- **Other**:
    - Given the variety of care settings, use cases and stakeholders that make up the care continuum it is not feasible at this time to put forth one “interoperability framework” that can accommodate each of these unique scenarios. A “minimum necessary” set of business, legal, privacy and technical protocols can be identified across these existing approaches, and leveraged to develop a baseline framework for trusted exchange. This baseline, similar to the Common Clinical Data Set, can simplify onboarding for participants, allowing for greater involvement across the disparate exchange solutions.

Cooperation and Non-Discrimination

- **General Reaction**: Respondents were broadly supportive of requiring cooperation and non-discrimination as a principle in the TEFCA to ensure that business competition does not inhibit the exchange of data. Some respondents noted the importance of ensuring the approach to cooperation and non-discrimination that ONC adopts does not contain loopholes that can be used to avoid exchanging data with business competitors.
- **Trust Arrangements Policies**: Many of the existing trust arrangements noted that they have existing provisions requiring cooperation and non-discrimination among their participants. The provisions vary across the arrangements.
    - One of the respondents also noted the importance of ensuring participants cooperation includes provisions related to the governance and operations of the trust arrangement.
    - One of the respondents also noted that the provisions should be structured such that participants who are engaged in similar types of exchange activities and who play a similar role in the data exchange must treat each other equally and not discriminate among similarly situated participants. This balances the need for equal treatment with the reality that networks will include many different types of participants that have different roles and are engaged in different use cases.
- **Sharing as the Default Expectation**: Some respondents encouraged ONC to take an approach that establishing the default expectation as one of sharing data.
- **Other**:
    - **Federal Policy Alignment**: A few respondents noted the challenge presented by varying federal requirements between HIPAA and 42 CFR Part 2 which creates industry confusion around when it is permissible to exchange information.
    - **Special Considerations for Federal Agencies**: A federal respondent noted that unique governmental missions and interests must be considered when developing such provisions and in looking at information blocking. For instance, DoD and VA place certain limitations on the exchange of patient data for national security purposes.
    - **Recommended Items to Include**: A few respondents noted specific items or provisions that should be considered:
        - Mutual commitment to assist the other party in fulfilling regulation obligation.
        - Clear confidentially protection for proprietary information.
        - A mechanism for stakeholder collaboration and dispute resolution.
        - Safe harbor provisions to address anti-trust and collusion concerns.
    - **Record Location Information**: A few respondents noted that there should be a clear core principle for purposes of treatment that such data can be shared within and across networks to enable participants to access/exchange those records within the confines of HIPAA and 42 CFR Part II. A provider or network should not prohibit or limit another network engaged in health information exchange to use relevant record location information to accurately and efficiently locate such records for treatment purposes.

Security and Patient Safety

- **General Reaction**: Respondents agree that security and patient safety is an important principle of the TEFCA.
- **Recommended Security and Patient Safety Areas of Focus:** Respondents suggested a number of areas of focus that should be addressed including:
  - Patient identification and authentication.
  - Break the glass provisions to allow for emergency access.
  - Require cyber liability insurance with a specific coverage amounts.
  - Leverage the All of Us Research Trust Principles and Data Security Policy Principles and Framework.
- **Patient Identification and Authentication**: A large number of respondents expressed concerns regarding patient identification/authentication, citing misidentification as a barrier to interoperability which directly impacts patient safety. A sampling of comments follows.
  - To elevate data integrity and patient safety ONC is urged to:
    - Advance patient record matching to verify the data belongs to the correct individual
    - Establish data review standards so inaccurate information in a patient record is identified and corrected, meets a legal standard to provide some assurance of accuracy and contains all necessary information, including metadata that provides a clearer picture of a patient's health record
  - Establish common identity proofing practices and requiring multi-factor authentication for all patients and providers.
  - For authentication, we note that Direct Trust, Car*e*Quality, the CommonWell Health Alliance, and the Surescripts National Record Locator Service (RLS) have existing technologies and frameworks that allow for scalable authentication of participants that ONC can look to and recognize as part of the TEFCA.
  - The burdens related to the various levels of identity management can differ significantly in terms of cost and level of effort, whatever is chosen must be flexible enough to be effective without being overly burdensome for either the user being authenticated or the entity charged with performing the authentication.
  - OAuth 2.0 and OpenID are currently the most widely accepted standards for internet security. We would like to see additional guidance as to how we can all make it easier for patients to authenticate while still preserving security.
- **Balancing Patient Safety and Security**: Respondents noted it is a balancing act to ensure patient safety and data security while providing access to clinical data at the point of care regardless of location. The goal of any exchange framework is that data should reside in the most secure environment while liquid enough to be available when and where needed.
- **Unauthorized Disclosures**: The TEFCA should recognize that an unauthorized disclosure of health information could potentially affect multiple participants. Statutory or regulatory notification obligations are not always clear when data is passing between covered entities via a chain of several business associates, participants should be required to notify each other of potential unauthorized access, use, or disclosure of message content so that all parties can fully determine their legal obligations.

- **Consumer Control over Data Flows**: With the introduction of the open APIs, patient use should not be limited by provider or developer imposed security and safety constraints. OCR, ONC, and FTC should work to help inform patients, providers, and health IT developers of their regulatory obligations and the risks of different approaches.
- **Information Governance**: A respondent noted all parties should be required to practice information governance, and the TEFCA should require that all parties practice information governance and hold their exchange partners accountable for ongoing comprehensive information governance practices.
- **Unique Federal Requirements**: ONC needs to collaborate further with other federal agencies to identify methods to ensure that the private sector adequately protects controlled unclassified information (CUI) that would be transmitted through their private sector exchanges or networks.
    - Any Common Agreement should include Cybersecurity requirements, such as NIST SP 800-171, that certain federal agencies are obligated to require private sector entities to comply with if they receive controlled unclassified information (CUI), such as ePHI, from that agency.

Access

- **General Reaction**: Respondents agree that access is an important principle for the TEFCA. While there was strong support for this principle, a number of respondents noted that networks and trust arrangements support different use case. While the overall framework should support access for the outlined parties certain components are out of scope for some networks and arrangements and should not be required of them through the TEFCA.
- **Recommended Access Components of the TEFCA:**
  - ONC should address national standards or other methods to address and resolve inconsistencies among states' laws regarding information access for minors, parents, and other surrogates.
  - Respondents are concerned about how ONC defines "easy" in the context of this principle. An incorrect or unclear definition could have significant downstream effects. Defined too leniently, ONC could inadvertently instantiate a significant security vulnerability in the national infrastructure that could be exploited by bad actors. Conversely, defined too stringently, by allowing local policy decision makers to create false barriers to exchange in the name of "system integrity," ONC could inadvertently stifle a significant amount of exchange that could otherwise positively impact patient safety and outcomes.
  - Credentialing and validating must be scalable. Developers will face unpredictable costs if they must individually validate every single application that seeks to integrate with a patient health record.
  - The TEFCA must be flexible and secure in providing access to information to the appropriate care provider at the point of care regardless of care location. The framework must accommodate patients, caregivers, and consumers who are demanding access to their information in a usable format for making informed health care decisions based on cost and quality.
- **Consumer Access**:
  - Some respondents noted the TEFCA should be leveraged to improve patient's access to their health information. A subset of these respondents requested that patients have low cost or free access to their health information through APIs.
  - Some respondents requested clarification of the use of "caregiver" in the context of this principle: does it refer to a patient's clinician, a family member or other designated care guardian, or both?

Data-Driven Choice

- **General Reaction**: Many respondents generally acknowledged the importance of this principle but this principle had the most push back in the comments. Some respondents noted that this principle is outside of the scope of the statutory language of Cures and recommended it not be included as part of the floor requirements in the TEFCA for all networks. Rather decisions to support or not support such use cases should be made at the network level.
- **Points of Clarification**: A few respondents requested clarification on what is intended by this principle:
    - What is the data set in scope?
    - What are the privacy considerations that drive what data needs to be de-identified or can remain identifiable?
    - Who can ask for that data?
    - How would this be supported/operationalized through policy/regulations?
    - What impact does this have on business models and the market?
    - What does "exchange multiple records at one time" mean (a source providing multiple documents for a source at one time or multiple records from multiple sources etc.)?
    - Are their different policies that apply to accessing data for this purpose?
- **Other**:
    - **Public Health**: ONC should encourage public health organizations to develop tools and processes for communicating information to public health agencies for public benefit, (e.g. providers may need access to DEA for Rx patterns from healthcare providers to identify opioid abuse.)
    - **Further Study**: ONC should charge the HIT Advisory Committee with providing recommendations on the public benefits and risks associated with the sharing of secondary data derived from a health record.
    - **Quality and Cost Transparency**: A number of respondents expressed a desire to be able to shop online for providers and medical services based upon cost and quality of care. A sample is below.