Comments on: DRAFT Trusted Exchange Framework – Common Agreement (TEFCA)

Source: US Department of Health and Human Services
Office of National Coordinator for Health Information Technology (ONC)

Date: 20 February 2018

Submitted by: CentriHealth, a subsidiary of United Health Group

Compiled by: Gary L. Dickinson
Director of Healthcare Standards at CentriHealth
Co-Chair, Health Level Seven (HL7) Electronic Health Record (EHR) Work Group

Thank you for the opportunity to comment on the proposed ONC "Trusted Exchange Framework – Common Agreement" (TEFCA).

General Comments

Our comments are compelled less by what DRAFT TEFCA contains and much more by what it lacks. It assumes that "trusted exchange" (indeed interoperability) is already in place and all we need to do is tie a bunch of EHR/HIT systems and HINs together to yield its full fruition. Somehow it conflates the success of driving provider adoption of EHR systems (via Meaningful Use, MACRA and related system certification programs) with the enduring deficiency of full health data/record interoperability among them.

1. Trusted Exchange Between Carer and Cared For

The proposal makes an error of interpretation common to nearly all strategic policies in this field, in the USA and elsewhere. It sets as its objective integrated *individual* care but pursues an approach based on integrated *institutional* processes. It equates "integrated institutions" with an "integrated individual". This always fails. The "trusted exchanges" we need are not between institutions, but between the carer and the cared for.

The health objectives of the proposal are stated in individual-centric terms. For example at the opening:

> *"The 21st Century Cures Act's (Cures Act) focus on trusted exchange is an important next step toward advancing the establishment of an interoperable health system that:*
>
> - *"Empowers **individuals** to use their Electronic Health Information to the fullest extent;*
> - *"Enables providers and communities to deliver smarter, safer, and more efficient [**individual**] care; and*
> - *"Promotes innovation at all levels."*

Similarly later on:

> *"The vision we seek to achieve is a system where **individuals** are at the center of their care and where providers have the ability to securely access and use health information from different sources. A system where an **individual's** health information is not limited to what is stored in*

*electronic health records (EHRs), but includes information from many different sources (including technologies that **individuals** use every day) and provides a longitudinal picture of their health."*

It then lists four important outcomes:

A. *"Providers can access health information about their **patients**, regardless of where the patient received care;*

B. *"**Patients** can access their health information electronically without any special effort;*

C. *"Providers and payer organizations accountable for managing benefits and the health of populations can receive necessary and appropriate information on **a group of individuals** without having to access one record at a time (Population Level Data), which would allow them to analyze population health trends, outcomes, and costs; identify at-risk populations [cohorts of individuals]; and track progress on quality improvement initiatives; and*

D. *"The health IT community has open and accessible application programming interfaces (APIs) to encourage entrepreneurial, user-focused innovation to make health information more accessible and to improve electronic health record (EHR) usability."*

There is nothing here that says the goal is to have hospitals integrated with doctors' offices and laboratories *per se*. And yet all the proposals for how to achieve the health care objectives are expressed in institution-centric terms. Health information exchanges (HIN) are themselves exchanges between institutions. The proposal here is for a 'HIN of HINs'. Hence all the discussion of agreements between institutions. The very need for such an overarching agreement is a reflection of the impossible many-to-many complexities of direct inter-institutional arrangements. Meanwhile, the individual remains scattered and fragmented across these structures.

This is a profoundly flawed conception of the problem and its solution, and one that has been proven repeatedly not to work at small scale, let alone at the scale and organizational complexity proposed here. The answer to tackling the complexity is not more of the same. The workings of institutions can no longer act as proxies for the experiences of an individual. The perspective on the problem needs reorienting.

2. With not About

The whole aim is to ensure individuals get coherent, "joined-up" care. That can only be achieved if the individual is the conceptual design center of our information infrastructure. Care is provided to individuals and hence information should align with that care. The trusted information exchanges and interoperability aren't required between institutions. They need to be between the individual and those proving them with care. Institutions need to stop talking *about* individuals and talk *with* them.

This requires a new class of infrastructure: an Individual Health Record (IHR) that is fundamentally designed to support the overall health and care of the individual across all providers and over extending time. The IHR is a persistent account of an individual's health and care, contributed to and used by all those participating in their care, with permission. It works with existing institutional systems such as hospital EHRs that will continue to manage the detailed intra-institutional processes. Those providing an individual with care should use and contribute to their IHR as part of their duty of care to the individual. An individual's IHR must be held on their behalf and used under the purview of a Custodian (new role).

This model dramatically simplifies the arrangements. In essence the IHR becomes the point of integration within the whole health system for that individual.

A. The IHR is a persistent account of what matters for an individual and is available for their care across providers and over extended time: the complexities of scattered records, brought together at some unspecified point in the future go away

B. The individual has a direct, complete way to access their own information and fully participate in their own care

C. Through the IHR it is possible to continuously monitor the individual's health and care to help achieve the intended health outcomes, regardless of whether or not a particular institution chooses to 'take a look'

D. The information agreement is between the individual and those providing care at the time of care, overseen by a custodian, and not between an indeterminate and mostly likely unknowable set of institutions.

E. It aligns privacy and confidentiality with the wider responsibilities and duty of care

F. There is a clear model for managing cohorts of individuals (populations): with appropriate agreement, a custodian can provide information on cohorts of individuals without requiring one-at-a-time access.

G. Innovation and access to application programming interfaces becomes a much simpler issue: work with the IHR to participate

All of these capabilities are exactly what the Act set out to achieve. They can only be realized by making individuals 'real' in our information infrastructure. The time to act is now.

[Comments continue on next page]

3. Essential Characteristics/Properties/Qualities of Health Data/Records resulting from Trusted Exchange

Let's start with trust (or "trusted" – the "T" in TEFCA). This is very basic, but let's be open and explicit about what "trust" and "trusted exchange" of health data/records really is. First, we should consider essential characteristics, properties and qualities of health data/records that are the vital result of "trusted exchange" and which must always and clearly be evident to the end user.

Essential characteristics of health data/records resulting from trusted exchange...		Properties/Qualities Evident to End User
A	Actionable in support of real-time care delivery	Timely, Concise, Pertinent, Digestible, Comprehensible
B	With known clinical context: e.g., problem/complaint/ symptom, diagnosis, treatment, protocol, status	Condition(s), Factor(s), Circumstance(s), Acuity
C	With facts, findings and observations regarding actions taken	Explicit, Specific, Cohesive
D	Associated with like information	Correlated, Comparable
E	Oriented in time: • What has happened (past, retrospective) • What is now in progress (present, concurrent) • What is anticipated, planned (future)	Chronological, Longitudinal
F	Oriented to actions taken: who did what when, where & why	Accountability, Transparency
G	Known and verified (verifiable) as to identity: • Subject: patient • Provider: individual and organization • Systems, devices and software	Identified, Attributed
H	Captured, consolidated from multiple sources	Integrated, Aggregated
I	Tuned for consistency: e.g., element names, data type(s), input/display/storage format(s), common units of measure, common vocabulary, common codes and value sets	Uniform, Congruent
J	Tied to the "source of truth", showing source and related details at point of data/record origination and at each point thereafter (including capture, verification/attestation, retention, transmittal, receipt, access/view...)	Factual, Authentic, Traceable
K	With known provenance	Source, Lineage
L	With known authorship, author's role and credential(s)	Ascription, Credence
M	Known to be unaltered since collection/origination	Immutable, Enduring
N	Known to be complete – or known to have missing elements	Whole or Partial
O	Known to be original – or known to be updated from original instance	Origin to Current Instance (data progression over time)
P	With measures/indicators (when appropriate) to show: • Quality, performance, outcome • Cost and value-based determinants	Efficacy, Effectiveness, Efficiency, Productiveness, Benefit

The described properties/qualities (right column) ensure that source and shared health data/records manifest:

- *Evidence of truth (authenticity);* as the
- *Basis of trust (assurance);*
- *For all end use(s) and to all end users.*

4. Ongoing Management/Assessment/Assurance Functions of Trusted Exchange

Let's now extend these same properties/qualifiers and apply them to "trusted exchange":

Essential characteristics of health data/records (from above)...		In the course of trusted exchange...
A	Actionable in support of real-time care delivery	Is actionable content captured, identified and conveyed?
B	With known clinical context: problem/complaint/symptom, diagnosis, treatment, protocol, status	Is full clinical context captured and conveyed?
C	With facts, findings and observations regarding actions taken	Are facts, findings and observations fully captured and conveyed?
D	Associated with like information	Are associations fully captured and conveyed?
E	Oriented in time: • What has happened (past, retrospective) • What is now in progress (present, concurrent) • What is anticipated, planned (future)	Is chronology fully captured and conveyed?
F	Oriented to actions taken: who did what when, where & why	Are actions and accountabilities fully captured and conveyed?
G	Known and verified (verifiable) as to identity: • Subject: patient • Provider: individual and organization • Systems, devices and software	Is identity and attribution fully captured and conveyed?
H	Captured, consolidated from multiple sources	Is it fully captured and conveyed?
I	Tuned for consistency: e.g., element names, data type(s), input/display/ storage format(s), common units of measure, common vocabulary, common codes and value sets	Is data element consistency fully captured and conveyed?
J	Tied to the "source of truth", showing source and related details at point of data/record origination and at each point thereafter (including capture, verification/attestation, retention, transmittal, receipt, access/view...)	Is the "source of truth" and traceability to that source fully captured and conveyed?
K	With known provenance	Is provenance fully captured and conveyed?
L	With known authorship, author's role and credential(s)	Are authorship, role and credentials fully captured and conveyed?
M	Known to be unaltered since collection/origination	Is unaltered source content fully captured and conveyed?
N	Known to be complete – or known to have missing elements	Is complete/incomplete status fully captured and conveyed?
O	Known to be original – or known to be updated from original instance	Are original content and successive updates fully captured and conveyed?
P	With measures/indicators (when appropriate) to show: • Quality, performance, outcome • Cost and value-based determinants	Are measures/indicators fully captured and conveyed?

In our opinion, there is nothing more important to the achievement of "trusted exchange" than rigorous stipulation (in the common agreement) that the essential characteristics/properties/qualities of trusted health data/records (as identified above) are consistently achieved, both in terms of the initial joining but also in ongoing management/assessment/assurance functions of all entities exchanging trusted health data/records. It is imperative that these characteristics/properties/qualities extend from the source, through exchange, to each end use and user. Nothing could be more critical. Otherwise there is little safeguard to prevent garbage in, then garbage out, and thus "distrusted exchange".

Measures to ensure qualitative assessment/assurance are far more important to "trusted exchange" than quantitative enumeration of transaction volumes, participating nodes, or volumes of data massed.

We believe TEFCA must include these specific provisions.

5. Basic Trusted Exchange Assessment 1 – Comparison Across Point(s) of Exchange

One basic form of trusted exchange assessment follows the pattern of collect, share and use.

Collect (at source of truth)	**Share** (exchange)	**Use** (if fit and trusted)
Input – Health data/records as collected (originated/retained)	= (identical) or ≠ (not)	Output – Health data/records as received, integrated and ready for use
What originated (began as)		What transpired (resulted in)
What the human (author) sees		What the human (user) sees
↑	**Assessment – Measures Results of Comparison**	↑

We believe TEFCA, as the over-arching framework for "trusted exchange", is incomplete without clarity and focus on the pattern of collect, share and use (from the ONC Interoperability Roadmap), to thus include a specific plan for initial and ongoing assessment – by comparison of health data/records at the point of collection/origination to those manifest (as fit for use) at each ultimate point of use, after being shared/exchanged.

6. Basic Trusted Exchange Assessment 2 – Comparison after Round-trip Exchange

A second form of "trusted exchange" assessment is based on a simple round-trip conveyance of health data/records...

System X	Exchange	System Y
A. Extracting from source health record entries, sends a clinical payload using any single or combination of exchange artifact(s)	→ → →	**B.** Instantiates payload in health record entries
D. Instantiates payload in a new set of health record entries	← ← ←	**C.** Extracting directly from those health record entries, sends the same clinical payload back using any single or combination of exchange artifact(s)
Assessment – Measures Results of Round Trip Exchange: Is there any loss of content, context, provenance, meaning or fidelity when comparing original System X record entries to System X record entries resulting from the round-trip (A + B + C + D)?		

Other Patterns: a) Reverse Roles of Systems X & Y b) System X → System Y → System Z → System X
Exchange Artifact(s): e.g., HL7 or NCPDP or X12 messages, HL7 CDA/CCDA documents, HL7 FHIR resources

We believe TEFCA, to provide initial and ongoing assurance of "trusted exchange", must also stipulate the requirement for round-trip exchange assessment of health data/records, following the pattern shown above.

[Note that Assessment 2 was developed in collaboration with the Health Record Banking Alliance (HRBA) and members of the US Technical Advisory Group (TAG) to ISO TC215.]

7. "Fitness for Use" and the End User's Affirmative Trust Decision

Regarding Comments 3-5 above, it occurs that these properties/qualities are the same as those that demonstrate truth (traceable to the source of truth) and enable an affirmative trust decision by the end user. In other words, if these properties/qualities are evident the end user can readily determine whether the health data/records presented are in fact trustworthy and "fit for use" in terms of the intended purpose (whether for primary or secondary use).

We believe fitness for use (of exchanged health data/records) and the affirmative trust decision (by the end user) are the vital result of "trusted exchange" and must be established as explicit TEFCA principles.

8. Trusted Exchange without an Actual Source of Truth?

As formulated in the DRAFT TEFCA, "trusted exchange" fails to start at (or even consider) the source of truth – the point where health data/record content is collected/originated. Given this neglect, it occurs that this specification misses the fundamental anchor point for successful interoperability and offers vanishingly little beyond a rehash of what is known (and well-proven) to have failed thus far.

9. Content Transformation in the Course of Trusted Exchange

As described in previous comments, achievement of interoperability must ensure fitness for use (purpose) at each ultimate point of health data/record access/use. The following table shows the challenging paradigm of health data/record exchange between heterogeneous systems and the risk to fitness (for use/purpose) posed by data transformations. Transformations typically occur at least twice during exchange from source/sender to receiver. *With an intervening HIN, data transformations may occur even more than twice in the course of end-to-end exchange.* At minimum, consider data transformation to/from exchange artifacts, including those required in HIPAA, US Meaningful Use and MACRA regulations – HL7 v2 and NCPDP and X12 messages, HL7 CDA/CCDA documents and now HL7 FHIR resources. See following table.

Use	**Purpose**	**Health Record Content Exchange**			**Post Exchange Fit for Use/Purpose?**
		Source	→ → →	Receiver	
Primary	Clinical Care, Interventions and Decision Making	Without Transformation (maintains/ensures fidelity to source)			**YES**
		With Transformation(s)			**Often NO**
Secondary	Most Everything Else	With Transformation(s)			**Sometimes**

For TEFCA to fully enable “trusted exchange”, ONC must address health data/record content transformation in the course of exchange and whether resulting information maintains/ensures complete fidelity to source information. Primary and secondary use are distinct and will have different thresholds of acceptance/acceptability regarding transformed content.

10. Trusted Exchange includes Trustworthiness of Health Data/Record Content

Under Meaningful Use and now MACRA, we’ve well demonstrated that a health data/record exchange scheme of standards-based messages and documents across multiple disparate EHR/HIT systems often achieves something far short of trustworthy interoperability. The required exchange artifacts are routinely created as odd assemblages of fragmented, disjoint data sets/elements and lack the full complement of clinical context, chronology, provenance, consistency, useful classification and comparability. For example, observe the typical real-time mash-up of CCDA-based patient summaries from multiple disparate sources inbound to a EHR system, subject to review and interpretation by an (often-overwhelmed) clinical user.

Given what is described in DRAFT TEFCA “trusted exchange”, there is scant evidence that these thriving points of failure will soon be overcome. Therefore we believe ONC should take careful focus on ensuring clinical context, chronology, provenance, consistency, useful classification are unambiguous, and combined with clear requirements, in this scheme of trusted exchange.

11. The Scatter Model (or the Achilles Heel of TEFCA)

The Achilles Heel of DRAFT TEFCA is its reliance on the “Scatter Model” AND the proposition that it may be possible to assemble a patient’s health data/records – in real-time – based on a broadcast query mechanism. While it may be possible to broadcast a query for patient information in real-time, it is not feasible to expect that the query will reach – and get – an immediate response from all EHR/HIT systems where such information may reside.

For any number of reasons, delays could be measured in minutes, hours or even days. Further, there is a strong likelihood that it will be impossible to identify all possible locations where the data – and type of data – might be found (and ultimately retrieved) based on the query. From a practical standpoint, the requesting entity/clinician will always be in the position that they don’t know what they don’t know. They also don’t know how long it might be reasonable to wait for query response(s).

[See Comments 1-2] How much better foresight ONC might have to focus on how to engage patients in individual health record (or health record bank) accounts where all their health data/records can be directed and captured, typically after each encounter, using the Meaningful Use required mechanism for view/download/transmit. This allows subsequent queries to be directed to one place – an Individual Health Record or health record bank account – maintained by a trusted organization and controlled by the patient (or their representative). We believe there are obvious and undeniable strengths to this approach versus what TEFCA proposes – typically known as the “Scatter Model”. See the following table and in particular the distinguishing advantages shown:

	Scatter Model (what TEFCA proposes)	Strengths of the Individual Health Record or Health Record Banking Approach
Basics	Patient data/records are managed across 10s and 100s of HINs and 1000s of EHR/HIT systems, each of which maintains/manages: • Trusted software and storage • Accountability, authentication, authorization (permissions, consents), access control, audit mechanisms • Some fragment of the patient record • Myriad pointers and indexes	A designated and secure system which is: • Patient-controlled and provider neutral • Maintained by a trusted organization And where: • The patient maintains an electronic account and address • Patient records can be functionally stored in one place • Patients can direct their individual health data/records after each encounter (using MU provision for view/download/ transmit)
Broadcast query	Query goes to 10s or 100s of HINs, then on to 1000s of EHR/HIT systems	Query is directed to one designated HRB organization and account for each patient
Query response	Response may be minutes, hours or days later, and thus: • You don't know what you don't know • You don't know how long to wait for response(s)	• Response is immediate • All relevant and permitted records are immediately available • You immediately know what you need to know
Access control	Managed within a complex lattice of provider and HIN permissions plus patient consent directives	Managed at a single point by each patient
Patient consent directives	Managed and kept current across 10s or 100s of HIN and likely dozens of providers	Managed at a single point by each patient

Specific Comments

DRAFT TEFCA, Page 3, Paragraph 1: "While the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 stimulated significant health information technology (health IT) adoption and exchange of Electronic Health Information with the goal of every American having access to their Electronic Health Information, the interoperability experience remains a work in progress."

12. Interoperability Assessment and Improvement

As stated above, "the interoperability experience remains a work in progress" and the question is whether entities and systems participating in health data/record sharing under TEFCA will substantively contribute to this progress. To this end, we believe TEFCA should include specific targets to improve the "interoperability experience" and a specific plan for assessment of each participating entity and system (source/sender → via network → receiver) as to its ability to meet or exceed those targets. These assessments should include the characteristics/properties/qualities of trusted health data/records as outlined in Comments 3-4, plus end-to-end (source to use) and round-trip assessments as specified in Comments 5-6.

DRAFT TEFCA, Page 3, Paragraph 1: "The 21st Century Cures Act's focus on trusted exchange is an important next step toward advancing the establishment of an interoperable health system that:
- "Empowers individuals to use their Electronic Health Information to the fullest extent;
- "Enables providers and communities to deliver smarter, safer, and more efficient care; and
- "Promotes innovation at all levels."

DRAFT TEFCA, Pages 18-19, Principle 4, Privacy, Security and Safety:
"Ensure that Electronic Health Information is exchanged and used in a manner that promotes patient safety, including consistently and accurately matching Electronic Health Information to an individual...

"Ensuring the integrity of electronically exchanged data is paramount to patient safety. When Electronic Health Information is exchanged, the promotion of patient safety begins with correctly matching the data to an individual so that care is provided to the right individual based on the right information...

"In addition to the importance of the integrity of demographic data elements, overall Electronic Health Information integrity is a key component of promoting patient safety in electronic exchange. Where possible, standard nomenclatures should be used and be exchanged in a data format that is consumable by a receiving system, such as the C-CDA or via FHIR Application Programming Interfaces (APIs). Further, Qualified HIN participants need to update individuals' clinical records to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another healthcare organization. Finally, Qualified HINs and their participants should work collaboratively with standards development organizations (SDOs), health systems, and providers to ensure that standards, such as the C-CDA, are implemented in such a way that when Electronic Health Information is exchanged it can be received and accurately rendered by the receiving healthcare organization."

13. Focus on Safety and Safe Exchange

As outlined in the DRAFT TEFCA statements above, we agree with the general approach to address key aspects of safety however it doesn't go nearly far enough. We believe what is suggested is more akin to dipping a toe in the ocean instead of taking a healthy swim.

Patient identity matching is crucial and as well as ensuring the "integrity of demographic data elements". Standard nomenclatures are ideal but when transformation of data content is required – from source representation to exchange artifact (e.g., message, document, resource) to HIN representation to receiver representation – errors, alterations and omissions often occur, disjoining health data/record content, context and meaning, and *introducing new safety risks*.

While it is important to recognize the "need to update individuals' clinical records to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another healthcare organization", the critical relationship between medications, allergies, problems, diagnoses, encounters, assessments, clinical decisions, diagnoses, orders, results, diagnostics, interventions, observations, therapies and care plans are often lost or become unrecognizable. Once again *safety risks are introduced* via exchange artifacts and exchange mechanisms.

We believe that to enable "trusted exchange", TEFCA must have provision to identify, track and provide real-time alerts for identifiable safety risks occurring in the course of health data/record capture and exchange.

We spent considerable time developing and refining Comments 3-6, specifically to ensure the integrity/safety of health data/records over the course of their lifetime and at specific points in their lifecycle (origination, retention, update, verification/attestation, transmittal, receipt...). We also participated in development of ISO/HL7 10781 EHR System Functional Model and ISO 21089 Trusted End-to-End Information Flows, both international standards, which specifically address management

of health data/records over the course of their lifetime and at particular lifecycle events. This is also true for the HL7 Fast Health Interoperability Resources Record Lifecycle Event Implementation Guide (FHIR RLE IG – balloted and published as part of FHIR STU-3 and now in ballot as part of normative FHIR Core Release 4).

In the interest of safety and safe exchange, we strongly urge ONC include normative reference to relevant sections of both ISO/HL7 10781, ISO 21089 and the HL7 FHIR RLE Implementation Guide in TEFCA.

14. Principles for Trusted Exchange and Interoperability

As we have advised in previous Comments, there are a number of issues bound to the objective to achieve safe and "trusted exchange" which are contingent on full interoperability. While we generally agree with the six "trusted exchange" principles in DRAFT TEFCA, we don't believe them to be complete as noted below.

Trusted Exchange Principle (TEFCA, pg 13)	Our Comments
Principle 1 – Standardization: Adhere to industry and federally recognized standards, policies, best practices, and procedures.	No comments
Principle 2 – Transparency: Conduct all exchange openly and transparently.	No comments
Principle 3 – Cooperation and Non-Discrimination: Collaborate with stakeholders across the continuum of care to exchange Electronic Health Information, even when a stakeholder may be a business competitor.	No comments
Principle 4 – Privacy, Security, and Patient Safety: Exchange Electronic Health Information securely and in a manner that promotes patient safety and ensures data integrity.	Expand data integrity in "trusted exchange" to included essential characteristics, properties and qualities of health data/records as specified in Comments 3, 4 and 15.
Principle 5 – Access: Ensure that Individuals and their authorized caregivers have easy access to their Electronic Health Information.	Expand easy access to include patient-mediated exchange. [See comments 1, 2 and 11]
Principle 6 – Data-driven Accountability: Exchange multiple records for a cohort of patients at one time in accordance with Applicable Law to enable identification and trending of data to lower the cost of care and improve the health of the population.	Not sure how the title "data-driven accountability" relates to what is described. Accountability is a much broader concept and relates to actions taken in support of individual health, provision of healthcare and corresponding documentation in health data/records. [See Comments 3, 4 and 15]
Principle 7 (new) – Certainty in Patient Identity Matching	Establish formal mechanisms, automated and with manual verification (as necessary), to ensure correct patient identity matching.
Principle 8 (new) – Targeted, Fit for Use and Actionable	Establish formal mechanisms to ensure exchanged health data/records are timely, concise, targeted, immediately actionable, relevant and fit for, specific users and uses.
Principle 9 (new) – Authenticity and Completeness	Establish formal mechanisms to ensure health data/records are verifiably authentic, complete with clinical content, context and provenance and maintain fidelity to source.

Trusted Exchange Principle (TEFCA, pg 13)	Our Comments
Principle 10 (new) – Affirmative Trust Decision	Establish formal mechanisms to ensure exchanged health data/records routinely achieve an affirmative trust decision for the intended end user and use.

DRAFT TEFCA, Page 4, Paragraph 2: "...Congress directed ONC to 'develop or support a trusted exchange framework [TEF], including a common agreement [CA] among health information networks nationally,' which may include:
"(I) a common method for authenticating trusted health information network participants;
"(II) a common set of rules for trusted exchange;
"(III) organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and
"(IV) a process for filing and adjudicating noncompliance with the terms of the common agreement."

DRAFT TEFCA, Page 7, Paragraph 1: "The Trusted Exchange Framework's minimum set of policies, procedures, and technical standards are intended to advance interoperability, particularly with these stakeholders, and enable them to use HINs to support the many use cases that are important to them and their patients (clients), including the exchange of data for Treatment, Payment, Health Care Operations (TPO), Individual Access, Public Health and Benefits Determination."

DRAFT TEFCA, Page 8, Paragraph 1: "We [ONC] believe that the proposed Trusted Exchange Framework supports the interoperability goal of reliable information flowing to enable communication among services that make use of Electronic Health Information, ultimately providing stakeholders with greater choice."

DRAFT TEFCA, Page 8, Paragraph 4: "We [ONC] believe that we can move quickly towards nationwide interoperability, but we recognize that we cannot achieve interoperability alone. We look forward to the health IT stakeholder community joining us on this journey."

15. Key Concepts, What We Anticipated and What We Found (in DRAFT TECFA)

In Comments above we have outlined vital characteristics, properties and qualities of trusted health data/records, interoperability assessment approaches, safety, safe exchange and key objectives, that are foundational to "trusted exchange" and must be given serious consideration. Following is an extensive enumeration of Key Concepts (in landscape table format), including "what we anticipated" and "what we found" (in DRAFT TEFCA). We believe the Key Concepts identified must be included in the TEFCA "common set of rules for trusted exchange", in the "organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur", and also in the "minimum set of policies, procedures, and technical standards [that] are intended to advance interoperability... and enable them to use HINs to support the many use cases that are important to them and their patients (clients)...", as stipulated in (II) and (III) and in the spirit of declarations above.

Comment 15 Table – Key Concepts, What We Anticipated and What We Found (in DRAFT TEFCA)

Key Concept(s)	What We Anticipated (as an explicit condition of trusted exchange)...	What We Found (if anything, often a divergent or unrelated concept)...
Accountability	Accountability as – • Ascribed for actions taken (e.g., clinical care, interventions, decision making) • Ascribed for actions documented • Ascribed for health data/record content	No mention of accountability for actions taken/documented or health data/record content, instead... • "Health Insurance Portability and *Accountability* Act of 1996 (HIPAA)", p 5, 26 • "Data-driven *accountability* for exchanging multiple records for a cohort of patients at one time... to enable identification and trending of data to lower the cost of care and improve the health of the population", p 13, 21 • "...Population Level requests... fundamental to providing institutional *accountability* for healthcare systems...", p 21
Action(s), action(s) taken	As in – • Evidence of clinical actions taken in support of individual health and provision of healthcare • Detailing who did what when, where and why	No mention of provisions to include evidence of actions taken, instead... • "The RCE will be expected to monitor Qualified HINs compliance with the Common Agreement and take *actions* to address any non- conformity with the Common Agreement...", p 9 • "...provide for appropriate remedial *action*...", p 28 • "Each Qualified HIN shall provide the following capabilities and take the following *actions*...", p 31 • "...a discriminatory manner means *action* that is taken or not taken with respect to any Qualified HIN, Participant or End User...", p 35, 44, 47
Actionable	As in – ensuring health data/records are immediately actionable upon receipt	No mention
Attribute, attribution, attributable	See "accountability"	No mention of attribution of health data/record content, instead... • "*Attributable* Cost: the Reasonable Allowable Cost of the *Attributable* Services", p 23 • "*Attributable* Services refers to both: (a) the services provided by a Qualified HIN that are necessary for the Qualified HIN to perform its obligations under the Common Agreement... and (b) the services and licenses (if any) that the Qualified HIN must obtain from a third party in order to enter into the Common Agreement...", p 23 • "Reasonable Allowable Cost: costs of a Qualified HIN that: (a) were actually incurred; (b) were reasonably incurred; (c) are either the direct costs of providing the *Attributable* Services or are a reasonable allocation of indirect costs of providing the *Attributable* Services...", p 29 • "Purpose of Use *Attribute*", p 32 • "Qualified HIN's *Attributable* Costs", p 36 • "SOAP-based requests shall convey the locally-authenticated user *attributes* and authorizations using SAML 2.0 assertions...", p 40 • "The End Entity certificate possesses a subject distinguished name *attribute* with a single common name component equal to the fully qualified domain name of the Listed End Point", p 42
Attest, attestation	As in – preserving relationship (binding) of attestation to health data/record content attested	No mention
Author, authorship	As in – preserving relationship (binding) of author/authorship to health data/record content authored [See Comments 3-4]	No mention
Chain of trust	As in – capturing/preserving/ensuring a full and traceable chain of trust for health data/record content from source to use (via exchange) [See Comments 3-4]	No mention of provisions to maintain a traceable chain of trust for health data/records, instead... • "An approved *trust chain* issues the End Entity certificate.", p 42

Key Concept(s)	What We Anticipated (as an explicit condition of trusted exchange)...	What We Found (if anything, often a divergent or unrelated concept)...
Context	As in – capturing/preserving clinical context of health data/record content from source to use (across exchange)	No mention of provisions to maintain clinical context of health data/record content, instead... • "EHI includes information that is accessed, exchanged, used or maintained in the *context* of the Trusted Exchange Framework...", p 3 (footnote) • "The terms 'health information,' 'health data,' and 'data' are synonymous in the *context* of the TEFCA and refer to all electronic health-related data for a patient.", p 4 (footnote) • "Adapter services are designed to transform message content or, in this *context*, transform unstructured data to structured and coded vocabularies...", p 16 • "EHI also includes electronic health data accessed, exchanged or used in the *context* of the Trusted Exchange Framework...", p 25
(Prevention/tracking of) Data alteration	As in – prevention/tracking of data alteration from source to use: in exchange or in translation/transformation of health data/record content	• "Procedures to ensure that EHI is not improperly altered or destroyed", p 38
Data authenticity, authentication	As in – ensuring capture and exchange of authentic, authenticated and/or authenticatable health data/record content	No mention of provisions for data authenticity or authentication, instead... • "...a common method for *authenticating* trusted health information network participants", p 4 • "...standards or technical requirements that ONC should specify for identity proofing and *authentication*", p 11 • "Common *authentication* processes of trusted health information network participants...", p 22 • "AALs: the *Authentication* Assurance Levels described in NIST Special Publication 800-63...", p 23 • "ATNA Integration Profile: the Audit Trail and Node *Authentication* Integration Profile...", p 23 • "OpenID Connect: an interoperable *authentication* protocol based on the OAuth 2.0 family", p 24 • "SAML (Security Assertion Markup Language): an open standard for exchanging *authentication* and authorization data between parties", p 29 • "Each Qualified HIN's security policy shall include the following elements to ensure appropriate access controls and user *authentication*...", p 39 • "...Access Control Markup Language (XACML) Profile for *authenticating*, administering, and enforcing authorization policies that control access to health information...", p 39 • "Each Qualified HIN shall *authenticate* individuals at a minimum of AAL2...", p 39 • "FHIR API-based transactions that require End User *authentication*...", p 40 • "Each Qualified HIN's SOAP-based servers shall conform to the connection *authentication* requirements as specified in the IHE ATNA Integration Profile for Transport *Authentication* Security. Each Qualified HIN using local *authentication* or federated *authentication* for SOAP-based requests shall convey the locally-*authenticated* user attributes and authorizations using SAML 2.0 assertions as detailed in the IHE XUA Profile.", p 40 • "Each Qualified HIN shall ensure that message exchanges are secured using TLS/SSL 1.2 X.509 v3 certificates for *authentication*, and X.509 certificates are used for *authentication* of all transactions.", p 41 • "Each Qualified HIN shall *authenticate* third party applications to the authorization server's endpoint...", p 41 • "Each Participant shall *authenticate* participating End Users and individuals...", p 45 • "Each Participant shall *authenticate* participating individuals at AAL2...", p 45 • "Each Participant shall be responsible for complying with the technical security policy requirements relating to *authentication*, identity proofing and individual authorization...", p 45 • "...each End User shall be required to *authenticate* at AAL2...", p 47
(Prevention/tracking of) Data errors	As in – prevention/tracking of data errors occurring in capture or exchange	No mention

Key Concept(s)	What We Anticipated (as an explicit condition of trusted exchange)...	What We Found (if anything, often a divergent or unrelated concept)...
Data integrity	As in – ensuring key characteristics, properties and qualities of trusted health data/records [See Comments 3-4]	Limited focus on provisions for full assurance of data integrity, indeed... • "Principle 4 – Privacy, Security, and Patient Safety: Exchange Electronic Health Information securely and in a manner that promotes patient safety and ensures *data integrity*.", p 13 • "Each Qualified HIN's security policy shall include the following elements to ensure *data integrity* of all EHI that it receives, maintains or transmits: (i) Procedures to ensure that EHI is not improperly altered or destroyed; (ii) Procedures to protect against reasonably anticipated, impermissible uses or disclosures of EHI; (iii) Procedures to maintain backup copies of systems, databases, and private keys in the event of software and/or data corruption, if the Qualified HIN is serving as a certificate authority; and (iv) Procedures to test and restore backup copies of systems, databases, and private keys, if the Qualified HIN is serving as a certificate authority, to ensure each Qualified HIN can retrieve data from backup copies in the event of a disaster, emergency, or other circumstance requiring the restoration of EHI to preserve *data integrity*.", p 38, 39 • "Each Qualified HIN shall report instances of inaccurate or incomplete EHI to the Participant who is the originator of the EHI, and request that Participant remediate such *data integrity* issues in a timely manner to the extent reasonably possible.", p 39
(Prevention/tracking of) Data loss, data omission	As in – prevention/tracking of data loss from source to use: in exchange or in translation/transformation of health data/record content	No mention
(Reduction of) Data Review Burden	As in – providing timely, concise, tailored, relevant and actionable health data/records for clinician review	No mention in terms of easing the burden of clinician review, instead... • "As the Fair Information Practice Principles (FIPPs) of the Nationwide Privacy and Security Framework on openness and transparency states, "[p]ersons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to *review* who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format.", p 20 • "As part of its ongoing security risk analysis and risk management program, this evaluation must include a *review* of the NIST CSF...", p 38 • "To the extent that a review of the NIST CSF HIPAA Security Rule Mapping identifies any gaps in the Qualified HIN's compliance with the HIPAA Rules or other Applicable Law...", p 38
(Reduction of) Documentation Burden and Fatigue	As in – facilitating reduced documentation burden on clinicians and practitioners (to improve usability)	No mention
(Reduction of) Duplicate(s), duplication	As in – removing duplicate health data/record content in the course of exchange and thus, reducing volume and improving concision and usability	No mention
Evidence, evidentiary support, proof, legal record, legal discovery	As in – • Ensuring health data/record content is captured, managed and exchanged according to requirements for a legal health record • Including need for use in legal discovery • Including evidence/proof of actions taken and source, authorship, attestation and verification of health data/record content	No mention in terms of evidence/proof in support of a legal health record, instead... • "Each Qualified HIN shall be responsible for taking reasonable steps to ensure that all Participants are abiding by the obligations stated in [the Participant Compliance] Section. Each Qualified HIN further shall require that each Participant provide written documentation *evidencing* compliance with these obligations on at least an annual basis.", p 46 • "A Qualified HIN's failure to incorporate the Common Agreement's terms and conditions into a Participant Agreement to the extent required herein shall be considered *evidence* of a material breach of the Common Agreement.", p 46

Key Concept(s)	What We Anticipated (as an explicit condition of trusted exchange)...	What We Found (if anything, often a divergent or unrelated concept)...
		• "A Participant's failure to incorporate the Common Agreement's terms and conditions into an End User Agreement to the extent required herein shall be considered evidence of a material breach of the Common Agreement.", p 47-48
Failure, failure conditions	As in – identifying points or types of failure conditions which may occur in the capture and exchange of health data/records	Limited focus on points or types of failure conditions in health data/record capture/ exchange, indeed... • "At a minimum, each audit record shall include the following information (either recorded automatically or manually for each auditable event): [i] the type of event; [ii] the date and time the event occurred; [iii] a success or *failure* indicator; and (where appropriate) [iv] the identity of the entity and/or operator that was responsible for the event.", p 43-44 • "In the event that a Qualified HIN becomes aware of a Participant's non-compliance with any of the obligations stated in this Section, then the Qualified HIN immediately shall notify the Participant in writing and such notice shall inform the Participant that its *failure* to correct any deficiencies may result in the Participant's removal from the Health Information Network.", p 46 • "Each Qualified HIN, each Participant of a Qualified HIN, and each End User acknowledges that the Recognized Coordinating Entity, other Qualified HINs, other Participants, and other End Users may report any *failure* to incorporate or to abide by the terms and conditions of the Common Agreement to ONC and/or the Office of the Inspector General...", p 46, 47 • "A Qualified HIN's [or Participant's] *failure* to incorporate the Common Agreement's terms and conditions into a Participant Agreement to the extent required herein shall be considered evidence of a material breach of the Common Agreement.", p 46, 47
Fit, fitness for use	As in – ensuring fitness for use of health data/record content: a) for intended purpose (e.g., clinical care, care coordination, claim for payment), b) within scope of intended receiver, c) as minimally necessary	No mention
Health record bank	As in – a designated, secure system which is: • Patient-controlled and provider neutral • Maintained by a trusted organization And where: • The patient maintains an electronic account and address • Patient records can be functionally stored in one place • Patients can direct their individual health data/ records after each encounter (using MU provision for view/download/transmit)	No mention
Legal health record	As in – designating all or portions of health data/record content as part of a formal legal record and providing full protection as such (including provision for legal hold)	No mention
Locally sourced versus externally sourced	As in – designating (and possibly segregating) portions of health data/records as locally sourced (within the domain of a specific provider) versus externally sourced (elsewhere)	No mention
Patient-mediated	As in – providing for patient-mediated exchange of health data/records	No mention

Key Concept(s)	What We Anticipated (as an explicit condition of trusted exchange)...	What We Found (if anything, often a divergent or unrelated concept)...
Patient-sourced	As in – ensuring patient-sourced health data/record content is clearly demarked and distinguished from clinician/provider-sourced content	No mention
Pertinent and relevant	As in – ensuring health data/record content is pertinent and relevant to the receiver and ultimately to the end user (e.g., clinician, practitioner)	Limited focus on tailoring health data/record content to specific receivers/users/uses, indeed... • "Part A of the TEFCA provides a set of core principles by which Qualified HINs—as well as all HINs—and data sharing arrangements for data exchange should abide. Specifically, these principles support the ability of stakeholders to access, exchange, and use *relevant* Electronic Health Information across disparate networks and sharing arrangements.", p 13
Primary use (e.g., clinical care, interventions, decision making)	As in – ensuring characteristics, properties and qualities of trusted health data/records to support primary use [See Comments 3-4]	No mention
Provenance	As in – preserving provenance relationship (binding) to health data/record content, at the message/document/resource, section and element level [See Comments 3-4]	No mention
(Trusted) record management domain	As in – • Designating health data/records as being sourced and initially managed according to the rules and processes of a trusted record management domain • Assuring essential characteristics, properties and qualities [See Comments 3-4]	No mention
Transformation, translation	As in – • Preserving original content and context when health data/records are transformed – from source representation to exchange artifact to receiver representation • Ensuring original text is carried alongside transformed content and context • Protecting against (and tracking) errors, alterations and omissions	Limited focus on preserving, protecting and tracking health data/record transformation and translation, indeed... • "Adapter services are designed to *transform* message content or, in this context, *transform* unstructured data to structured and coded vocabularies, so that Qualified HINs can exchange data with other Qualified HINs in a standardized format.", p 16 • "Qualified HINs and their participants should provide accurate *translation* and adapter services to their End Users to enable them to map proprietary data to standard, user friendly vocabularies.", p 16
Truth, source of truth	As in – ensuring, preserving and designating known source of truth for health data/record content	No mention
View, download, transmit	As in – the provision of Meaningful Use where certified EHR/HIT systems must enable a patient to view, download and transmit their health data/records to a designated system, entity or electronic address (e.g., following each encounter)	No mention