XpressRules—FEi:

XpressRules LLC and FEi Systems, large scale health IT solution providers as well as experts in interoperability standards and Meaningful Consent, are pleased to submit their combined comments in response to Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2.

Reference[1]	TEFCA2 Text	Comment
ExecSummary:4	ONC has focused on three high-level goals: • Provide a single "on-ramp" to nationwide connectivity. • Enable Electronic Health Information to securely follow the patient when and where it is needed. • Support nationwide scalability	These goals are significantly important and great to see that ONC is focusing on these. TEFCA has potential to take the nationwide connectivity and interoperability to the next level. However, there are significant challenges that need to be factored in, primarily in reference to differences in specialty health domains (e.g. BH and LTSS) as well as patient's ability to provide consent and preferences to control exchange of his/her EHI.
Intro:6	ONC received more than 200 public comments from stakeholders across the industry, including individuals, health care systems, payers, purchasers, care providers (e.g., long-term and post-acute care, behavioral health, community-based and safety net providers, …	TEFCA DRAFT 1 indicated concerns about interoperability amongst and with specialty domains such as BH and LTSS. However, those concerns are not mentioned or addressed in this DRAFT. Although DRAFT 1 had acknowledged concerns regarding interoperability for LTSS, BH and other ambulatory services, it did not provide specific steps/guidance to address that. Those were very legitimate concerns that are yet to be addressed to achieve interoperability across all domains and care settings and can't be undermined.
Intro:7	ONC has focused in on three high-level goals: 1) **Provide a single "on-ramp" to nationwide connectivity:** . . .	Providing single "on-ramp" is one of the most important goal for TEFCA. It has been challenging for many organizations to decide which network to be connected to if there are choices. Often there is no choice but to join only local network available and locked into it. Even though TEFCA may not necessarily result in increasing network choices locally, it will make it easier to connect to specific HIN and implicitly be connected to nation-wide network of HINs. But this needs to factor in specialty domains such as BH and LTSS as mentioned earlier since those systems may not be using the same standards

[1] Section number (or section title), followed by a ":", followed by the page number in *Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2*

		as primary health. This can be possibly be alleviated by establishing HINs that focus on those specific domains and provide add-on capabilities to overcome those challenges. For example, BH domain specific HIN can have stronger consent-based capability to comply with 42 CFR Part II to make it easier for BH providers to join.
Intro:9	• **Minimum Required Terms and Conditions (MRTCs) . . .** • **Additional Required Terms and Conditions (ARTCs):** . . .	It is not very clear why ARTCs have to be separate from MRTCs. As per the description, ARTCs will be essential part of the T&C for QHIN to meet. If they are mandatory T&C for all QHINs to follow, then these might as well be included as part of MRTC to avoid unnecessary confusion.
Intro:10	Stakeholders have the option of fulfilling the responsibilities for and participating as a QHIN, a Participant, a Participant Member, or an Individual User, each of which is explained in more detail below.	It is certainly good intent to have any of these stakeholders to join as a QHIN, a Participant or a Participating Member. However, it may be impractical or may be potential conflicts for certain types of stakeholders to be designated as QHIN (e.g. Individuals, Federal Agencies or Health Plans). Although this would be governed by MRTC, there may be a need for certain qualifying criteria for a stakeholder to become QHIN.
Intro:12	RCE approves or rejects HIN's QHIN Application	ONC needs to make sure that RCE's decision for QHIN application is solely based on well-defined decision criteria and checklist. Therefore any potential conflict or bias do not come into picture in making such a decision.
Intro:14	• **QHIN Message Delivery:** . . . (sometimes referred to as a "push").	"Push" notification generally should be based on subscription model based on patient provider attribution since QHIN should not deliver EHI to any QHINs or participants unless those receiving organizations have something to do with that patient. There is not much detail here regarding that.
Intro:14	**Exchange Purposes**	This term "Exchange Purposes" is better than "Permitted Purpose" used in DRAFT 1.
Intro:17	**Meaningful Choice**	We understand Patient-Centric "Meaningful Choice" as (1) the patient's own expression of privacy preferences as a policy for how her EHI is to be used (or not) and disclosed (or not) and (2) the enforcement of those immutable preferences in every disclosure of her EHI. Simply put, "Meaningful Choice" is enforcement of the patient's *intentions* and *expectations*, not just compliance with what the statutes allow or disallow.
Intro:17	**Written Privacy Summary**	We consider the ONC's 2018 Model Privacy Notice (MPN) as a basic requirements template for eliciting the patient's privacy options.
Intro:17	Participants and Participant Members are responsible for communicating this Meaningful Choice up to the	This calls forth "longitudinal consent": enforcement of the patient's Meaningful Choice in strict accordance with her immutable policy throughout the life cycle of her EHI.

	QHIN who must then communicate the choice to all other QHINs. This choice must be respected on a prospective basis.	
Intro:19	**Security Labeling**	Traditional practice of Security Labeling is (1) static (relying solely on most recent VSAC versions) and (2) "bespoke" (pre-defined). Challenge is to reconcile forward-looking real-time transactions (and analytics, hopefully) with a static framework.
Intro:19	ONC is considering the inclusion of a new requirement regarding security labeling . . .	Our position is that these rules MUST be included in the TEFCA, or not all data will be able to be transferred, thus creating significant clinical risk and inaccurate patient records.
Intro:19	• Any EHI containing codes from one of the SAMHSA Consent2Share sensitivity value sets for mental health, HIV, or substance use in Value Set Authority Center (VSAC) shall be electronically labeled;	We maintain that VSAC-based labeling alone--even if automated and rigorous--can only achieve *regulatory* compliance. This legacy approach cannot support access control decisions that truly fulfill the *patient's expectation*. This is because many "sensitivity clues" in the EHI reside (1) in unstructured notes and (2) among scattered terms in non-obvious relationships. Fulfilling the patient's expectation therefore clearly requires natural language processing (NLP) solutions. Development of (1) auto-detection of non-obvious sensitive data and (2) auto-marking of the EHI is currently underway at XpressRules, funded by a NIST cooperative agreement. Such auto-detection and auto-labeling are based on the patient's own identification of sensitive data, as required by 42 CFR Part 2.
Intro:19	. . . a new requirement regarding security labeling that states the following [5 bulleted labeling requirements]	We suggest these additional labeling requirements: • While the VSAC is the governing sensitive data set, patients shall be able to add to, or remove requirements from this data set for their personal data transference. • Patients shall be allowed to identify the external entities (caregivers, physicians, payers, etc.) that are able to see their information. • This information must be included in the highest document or security level
Intro:19	• Any EHI containing codes from one of the SAMHSA	SAMHSA's valueset serves as master reference of some key sensitivity categories and related to concept codes from major terminologies including SNOMED-CT, LOINC,

	Consent2Share sensitivity value sets for mental health, HIV, or substance use in Value Set Authority Center (VSAC) shall be electronically labeled;	RxNorm, ICD, CPT, etc. This is accessible to any organization that intends to use this valueset. Learning from this approach, it will be great to have such a centralized place for maintaining other value sets and other metadata needed under TEF. While HIN's, QHIN's, and participants must abide by this sensitive data list, patients should be allowed to add to or remove from this list for their personal medical record transference/consent.
Intro:19	• At a minimum, such EHI shall be electronically labeled using the confidentiality code set as referenced in the HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P)	It is great to see specifics on DS4P IG that is aligned with the Interoperability Rule.
TEF28	For example, for some health conditions such as human immunodeficiency virus (HIV), mental health, or genetic testing, . . .	It will be good to clearly state that consent is Part II-compliant when BH (or SA to be more specific) providers are likely to be part of exchange network. At a minimum, general designation should be made required to enable BH providers to participate in exchange network. This is essential to address lack of BH participation in the current HIEs.
TEF:29	**Principle 5 – Access: Ensure that Individuals and their authorized caregivers have easy access to their EHI.** . . .	Same comment as DRAFT 1: This requirement is still not addressing the issue/challenges that patients face in the current environment since access to their information is segregated. Each provider and/or EHR system provides access to their own data via tethered PHR or provides a summary document to the patient. It is not easy for the patient to get all of the information harmonized/integrated for each access. TEF should address this by enabling the patient to access all data from single point (even though it may require broadcast query on network to dynamically collect that information and provide to the patient).
TEF:29	HINs should commit to following this principle and should provide such opportunities electronically whenever possible, particularly when an individual makes the request electronically	Same comment from DRAFT 1: This text ("whenever possible") make it sound like providing a list of access/disclosures is an optional activity. But for BH information exchange under 42 CFR Part II General Designation, this is *required*. Ideally this should be a standard requirement for *all* disclosures to ensure that patient has visibility to who is getting/accessing his/her data.
MRTCs §4.1.2:46	"Fee Schedule. Within thirty (30) calendar days after signing the Common Agreement, each QHIN shall file with the RCE a schedule of Fees…"	Fees would generally depend on level of participation that may not be known early on. Although this requirement does not explicitly ask for fixed fee, it may be good to indicate possibility of variable fee structure.

MRTCs §6.2.1(ii):50	…protection of CUI on at least an annual basis, . . . comply with the security requirements of the then most recently published version of the NIST Special Publication 800-171	Title of the SP: "Protecting Controlled Unclassified Information (CUI) in non-Federal Systems and Organizations," which includes applicable section: §3.1 "Access Control" (15 subsections). As our implementation authority for access control we cite NIST SP 800-178 re "Next Generation Access control (NGAC)"
QTF:70	However, the QTF Draft 1 intentionally does not specify standards QHINs must use for these internal-QHIN implementation decisions.	Although specific standards are mentioned in this QHIN Technical framework, it is still relatively open-ended. If implementers choose whatever standard they prefer for specific capability, it is likely to have a negative impact on the interoperability needed through TEF. For example, HIE participants will continue using IHE-based transactions with C-CDA documents for exchange, while EHRs participants on the same or other QHINs may prefer to use FHIR. Multiple methods of communication (RESTful API in FHIR vs. SOAP web services in IHE transactions) as well as multiple content IG (FHIR profile vs. CDA-based IG) will make interoperability a lot more challenging, especially when there is mapping involved between various content standards. While keeping it more flexible makes sense for initial buy-in, ONC must establish a roadmap to converge to the standards that provide best interoperability with lower costs and technical hurdles.
QTF:77	Table 5. Specified & Alternative Standards for User Authentication	While IHE XUA focuses more on SAML-based authentication, more modern technologies rely on OAuth 2.0 and Open ID Connect (e.g. SMART-on-FHIR). So it is essential to specify all applicable standards here as opposed to limiting to just XUA. Also there should be a roadmap to use one of those more prominently over time (say Open ID Connect/OAuth2).
QTF:83	• A QHIN MUST be capable of accurately resolving requests to match patient demographic information with patient identities under its domain	This will likely be one of the most challenging problems to solve, not just within QHIN but across all QHINs. ONC must provide more specific guidance and a common solution/ algorithm for the patient identity and matching. Can ONC leverage the outcome from the earlier challenge (https://www.hhs.gov/about/news/2017/11/08/hhs-names-patient-matching-algorithm-challenge-winners.html)?
QTF:83	* ONC Request for Comment #7: …Should QHINs use a broader set of specified patient demographic elements to resolve patient identity . . .?	Set of minimum demographics information is certainly required. However, those data elements may have some typos and errors. So a heuristic algorithm around those characteristics will be needed (as opposed to literally matching those data elements).
QTF:83	* ONC Request for Comment #8: … should the QTF specify a single standardized approach to	Patient identity resolution model should rely on how QHINs are organized and connected. In other words, it is better to have patient identity resolution be at the QHIN level and used in a federated model as opposed to a centralized model. However, the

	Patient Identity Resolution across QHINs?	resolution should rely on a standardized set of data elements and an algorithm that may be centrally made available for all QHINs to use.
QTF:83	"Individuals whose EHI is available through the QHIN Exchange Network can choose to opt-out of further use and disclosure of their EHI through the network altogether by exercising Meaningful Choice."	Ability for individual to provide privacy preferences should be beyond just the opt-in and opt-out that HIPAA has adopted. That black-and-white approach does not provide flexibility to the individual/patient to be able control their information and share as needed. 42 CFR Part 2 is mentioned earlier in the rule. Even though not all aspects of the 42 CFR Part 2 is needed for all EHI, there are essential components of 42 CFR Part 2 consent that provide tremendous flexibility to individuals (e.g. ability to control sharing to specific providers or specific sensitivity categories). While QHINs provide nationwide connectivity for better service, there must be a higher obligation to respect the patient's privacy. Therefore more fine-grained consent preferences should be made required as opposed to plain opt-in/opt-out model for any EHI.
QTF:84	"Standards to address privacy preference include the IHE Basic Patient Privacy Consents (BPPC) Profile,…"	IHE BPPC has been superseded by HL7 CDA Consent Directive IG and FHIR Consent Resource Profile IG.
QTF:85	* ONC Request for Comment #13: In addition to enabling Meaningful Choice, the Common Agreement requires QHINs to collect other information about an **Individual's privacy preferences such as consent, . . .** [1] Should the QTF specify a function to support the exchange of such information through the QHIN Exchange Network? [2] Which standards and/or approaches should the QTF specify for this function?	1. We strongly urge for the specification of such a function (for information exchange), such "specification" to be in the form of a Guidance and or Implementation Guide. 2. We note that "consent" occurs 20 times in this document, invariably in the context of *statutory compliance*. But maturing global standards and approaches now provide a road map to *patient-centric* consent that is robust, auditable and enforceable. Under its NIST cooperative agreement XpressRules is engaged with London-based Open Consent Group to apply *consent by design* and to implement standardized *consent receipts*.[2] This addresses a current gap in the workflows for Code of Federal Regulations (CFR) 42 part 2 and is relevant to the International Organization for Standardization (ISO) and the General Data Protection Regulation (GDPR). We hope that this will encourage every player toward *standards-based* Meaningful Choice.

[2] Kantara Initiative *Consent Receipt Specification* 1.1.0 (2/20/2018)

XpressRules—Open Consent:

Combined XpressRules' and OpenConsent response to the ONC's request for comments to TEFCA2

ONC Request for Comment #13: In addition to enabling Meaningful Choice, the Common Agreement requires QHINs to collect other information about an Individual's privacy preferences such as **consent**, approval, or **other documentation when required by Applicable Law**. Should the QTF [QHIN Technical Framework] specify a function to support the exchange of such information through the QHIN Exchange Network? **Which standards and/or approaches should the QTF specify for this function** [bolding added]?

"Role and Relevance of (Consent) Receipts"

A substantial body of work over the last 7 plus years has focused on the role of receipts as a means of changing, for the better, the way people participate in the use of their subsequent personal information, and their contextual identification, characterization, and engagement. This work continues to progress in several standards organizations including: The Kantara Initiative, the W3C, OASIS COEL as well as by ISO. The Kantara Consent Receipt Standard has been adopted as a building block in building advanced privacy and security systems where the Meaningful Choice is made operational through legally established privacy rights and requirements. It is also in the process of being adopted as an appendix to ISO 29184 "Online privacy notices and consent".
https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification

The use of a receipt addresses ***all*** of Principles for Trusted Exchange call out for "The Trusted Exchange Framework".

- **Principle 1 – Standardization:** Adhere to industry and federally recognized standards, policies, best practices, and procedures.
- **Principle 2 – Transparency:** Conduct all exchange and operations openly and transparently.
- **Principle 3 – Cooperation and Non-Discrimination:** Collaborate with stakeholders across the continuum of care to exchange EHI, even when a stakeholder may be a business competitor.
- **Principle 4 – Privacy, Security, and Patient Safety:** Exchange EHI securely and in a manner that promotes patient safety, ensures data integrity, and adheres to privacy policies.
- **Principle 5 – Access**: Ensure that individuals and their authorized caregivers have seamless access to their EHI.
- **Principle 6 – Population Level Data:** Exchange multiple records for a cohort of individuals 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.

XpressRules and OpenConsent have outlined and drafted notice receipts that cover each of these categories. And while a receipt for (explicit) consent has many benefits so do receipts for other purposes. Importantly receipts provide not only transparency but also a means of engagement, in a balanced way, with individuals so that they can exercise their rights under a given jurisdiction, purpose and justification.

The use of receipts sets the stage for advanced security and privacy solutions. It combines transparency and user control with the operational goals of integrity, confidentiality and availability and does so in a way that can be common across QHINs, Participants and Participant Members and again very importantly for and from the perspective of individuals and they hold the receipt documenting actions, agreements and interactions greatly advancing the needed trust in the TEFCA Draft 2.

The use of receipts can greatly advance and address:

- **Meaningful Choice and Written Privacy Summary**
- **Breach Notification Requirements**
- **Minimum Security Requirements**
- **Security Labeling**

And the receipt is designed and being leveraged by many of the groups mentioned in the Alternative / Emerging Standards /Profile in particular HL7 FHIR RESTful API.

A critical component of the existing receipt is the ability to incorporate purpose. In this case we have (as an example) adopted the updated purpose categories in Draft 2.

- **Treatment**
- **Quality Assessment and Improvement**
- **Business Planning and Development**
- **Utilization Review**
- **Public Health**
- **Benefits Determination**
- **Individual Access Services**

And in the same way the ONC Model Privacy Notice can be adopted and incorporated as a profile/extension of the evolving standard.

In doing so we would show how it improves the Message Delivery Functions in the QHIN Exchange Network. In particular a receipt can play a key role in:

- **Authorization and Exchange Purpose**
- **Message Delivery**
- **Auditing**

Completion of XpressRules' NIST Cooperative Agreement, which includes OpenConsent as sub-contractor, will demonstrate how the Consent Receipts capability is being accomplished and can be further extended in concert with Draft2.

"OPN Network and Consent by Design"

While consent is not always a requirement under HIPAA, e.g

> The HIPAA Privacy Rule generally does not require covered entities to get an individual's consent or authorization before using or disclosing ePHI for treatment, payment, and health care operations purposes. While the Privacy Rule generally permits covered health care providers to give individuals the choice as to whether their health information may be disclosed to other covered entities or that covered entity's business associate for those purposes, some federal and state laws require health care providers to obtain an individual's written consent before they disclose or exchange an individual's EHI to other people and organizations, even for treatment and payment purposes. For example, for some health conditions such as human immunodeficiency virus (HIV), mental health, or genetic testing, state laws generally impose a more stringent standard (e.g., requiring consent from the individual) than HIPAA. Additionally, under 42 CFR Part 2, subject to certain exceptions, federally assisted "Part 2 programs" (certain substance use disorder treatment programs) are required to obtain an individual's consent to disclose or re-disclose health information related to substance use disorder information, such as treatment for addiction.
>
> Page 28TEFCA Draft 2

it is still the fact that notice and transparency need to be built into the operational principles regardless of purpose and justification. In addition to the use of receipts OpenConsent has also created a data controller registry that can be used to enroll and maintain a scalable, user-friendly and dynamic signal of the legal business entity and its privacy (and security) state. This complements some of the security features envisioned in Draft 2 around public key infrastructure with a like ability to monitor and broadcast the privacy equivalent of certificate status, certificate policy and associated object identifiers. We do this by focusing on privacy policy (company and service), privacy point of contact, identification of high risk, and state of business ownership as part of the controller registration. We refer to the registry as the OPN Network (as in Open Network) and create an icon that represents privacy and legal entity state (it could include TEF adherence), which when "clicked" provides multiple operational privacy features including the use of receipts

mentioned above. "Consent by Design" is our reference to the design and operation system protocol we use when building advanced privacy and security system such as that being constructed and envisioned for use in accordance with Draft 2.