patientprivacyrights

Patient Privacy Rights Comments to TEFCA Draft 2

TEFCA will succeed where previous national health information exchange efforts have failed only if it puts patients' and families', and/or their fiduciary agents, in control of health technology. This is the only path to restore trust in physicians, and to ensure accurate and complete data for treatment and research.

As physicians and patient advocates, we seek a longitudinal health record, patient-centered in the sense of being independent of any particular institution. An independent health record is also essential to enhancing competition and innovation for health services. TEFCA Draft 2 is the latest in a decade of starts down the path to an independent longitudinal health record, but it still fails to deal with the problems of consent, patient matching, and regulatory capture essential for a national-scale network. Our comments on regulatory capture will be filed separately.

We strongly support the importance in Draft 2 of Open APIs, Push, and a relationship locator service. We also strongly support expanding the scope to a wider range of data sources, beyond just HIPAA covered entities in order to better serve the real-world needs of patients and families.

However, Draft 2 still includes design practices such as the lack of patient transparency, lack of informed consent, and a core design based on involuntary surveillance. This institution-centered design barely works at a community level and leaves out many key real-world participants. It is wishful thinking to believe that it will work with expanded participant scope and on a national scale.

TEFCA's path to a successful national-scale network goes through the patient.

A person-centered architecture for health interoperability should emulate the modern-day version of our architecture for financial interoperability. Specifically:

- Data moves only with complete transparency under explicit patient authorization.
- The APIs are symmetrical with respect to read and write, push and pull.
- Security is enhanced by contemporaneous notification of all transactions.
- Surveillance, to provide a relationship locator service, is very limited and transparent.
- Coercive and probabilistic patient matching is replaced by voluntary identification linked to consent.
- Privacy by default is not only compatible with flow of sensitive data and social determinants of health, it's the only way patients will trust revealing this data .

Our detailed comments below call out where Draft 2 deviates from a patient-directed design and suggests the only scalable and sustainable alternative for data exchange. Page references are to Download the Trusted Exchange Framework and Common Agreement Draft 2.

Page 14 - Three exchange modalities
TEFCA should enable a longitudinal health record controlled by patients. From that perspective, it ensures patients know where their records are, ensures providers can get information from whatever places patients allow, and enables providers to update the patient record, with strong support for security and accountable attribution. All three modalities are essential to serving patients and health professionals. We recommend greater focus on the desired outcomes and guidance on how the modalities support the clinical outcome of patient-controlled care.

Page 15 - Individual Access Services
Individual access services are essential for a scalable network that also includes non-HIPAA entities. We recommend that TEFCA build on individual access to explicit consent mechanisms instead of HIPAA T/P/O, that TEFCA account for all disclosures, provide contemporaneous notice of all transactions, and build trust through this unified user experience. Just as TEFCA aims to present “a single on-ramp” to institutions, it should also provide a single point of contact for patients by linking consent and accounting for disclosures to a single point of contact that’s linked to the relationship locator service functionality in TEFCA. It’s time to give patients technology that makes it easy for them to easily navigate, understand, and control their health data.

Page 16 - Non-HIPAA entity participation
We encourage participation by non-HIPAA entities as well as HIPAA entities that are more strictly regulated under 42CFR Part 2. However, the draft description of how this will come about is too vague to be useful in terms of security as well as privacy. HIPAA is inadequate in many ways for 21st Century technology and practice because it avoids consent, transparency, and notice that is common practice in banking, telecommunications, and other networked services. We recommend that this section be rewritten without reference to HIPAA.

Page 17 - Meaningful choice to participate
This section is inadequate. Meaningful choice must be defined in terms of the patient, family, and physician experience. Should our choice be only all-or-none? Should what shows up as a result of broadcast queries or other relationship locator services be hidden from patients? Will patients be notified of all activity under TEFCA? How will patients manage dozens of service relationships including non-HIPAA and 42CFR Part 2 sources unless new technology to support patient’s/or a fiduciary agent’s easy management of our health data? Will patients have the opportunity to specify a particular QHIN of their choice as primary access providers?

Page 19 - Security

Transparency and contemporaneous notification of activity is essential to modern network security. Draft 2 fails to provide adequate guidance of how this will be achieved.

Page 19 - Individual rights
We commend Draft 2 for being explicit on the primacy of individual rights and urge further clarification of how users can exercise their individual rights.

Page 20 - No charge for individual access services
This is an essential component for a successful network. A QHIN that wants to compete on the basis of individual access services must be able to provide patients and physicians a defined fee structure regardless of where the information originates.

Page 26 - HIN privacy practices
This section is confusing. The requirements for patient-directed sharing are pretty clear in the recent ONC NPRM with regard to covered entities. The underlying assumption is patients should have a choice of covered entities. Will patients have a choice of HIN? Will patients even know which HIN has information about them? We support patient-directed sharing as the foundation for TEFCA but seek clarity and technology standards to assure it works from the patient and physician perspectives. We suggest more specific solutions below.

Pages 28 and 29 - Patient-directed exchange
We strongly support a TEFCA design built on patient-directed exchange via APIs. As mentioned above, this is the only method that can solve consent and patient matching problems at scale. Nothing else is scalable.This section is a good start because it makes explicit that the introduction of HINs (and QHINs) should not dilute or limit the patient experience via technology or limit the scope of patient-directed access. From a patient perspective, will patients have a choice of HINs? Will QHINs compete with HINs? How will patients know or choose where to address their requests for patient-directed sharing: to a covered entity, a HIN, or a QHIN?

Page 45 - Patient matching
Moving around patient demographic data for patient matching purposes is a national surveillance mechanism of unprecedented scale outside of law enforcement. Once it becomes public, it will spook many patients and cause them to opt-out of TEFCA all together. Building TEFCA on a surveillance backbone will limit both the kinds of patients who will participate and the kinds of services that they will connect with. Furthermore, the whole framing of this section makes clear that mistakes in patient matching will happen. What will be an acceptable threshold for errors? How will patients become aware of the errors? Who will be responsible for fixing the errors?

Page 51 - Identity proofing
HIPAA allows treatment on the basis of “known to the practice”. Although QHINs are not a covered entity in the treatment sense, the requirement for identity-proofing means patients who receive care under “known to the practice” will not be able to participate in TEFCA. We urge

HHS to make TEFCA accessible to all patients by allowing patients to self-identify (as part of the consent process) if they choose. Identity-proofing in healthcare is only appropriate under very limited circumstances such as prescribing of controlled substances. Typical care, including third-party payment, can be done as known-to-the-practice and to the payer without introducing privacy compromises on a national scale.

Page 69 - Accounting of disclosures exception
Section 9.5.3 violates good security practice and should be unacceptable for a national-scale government program. Lacking transparency, a TEFCA built on hidden transactions and national-scale surveillance will not be trusted by many patients. As of 2016, 89% of patients are withholding information from providers. Computation and connectivity are now effectively universal and must be leveraged by TEFCA to the fullest extent in order to provide security, engender trust, and catch errors.

Page 82 - Direct address and other address modalities
The ability to correctly designate a recipient is essential for both patients and clinicians. National databases such as NPPES (for NPI) and Physician Compare that already exist and they are open for access in order to verify the identity of a designee. We urge TEFCA to build on this existing infrastructure by adding Direct addresses to NPPES and Physician Compare. To the extent that TEFCA develops other means of identifying practices or individuals, we strongly urge them to be fully open, API-enabled, and easily accessible to products and services in the general marketplace and beyond TEFCA.

Page 85 - ONC Request for Comment #7 - Patient matching
The E in IHE stands for Enterprise. Patient matching at enterprise scale is complex but uncontroversial because the patient universe is relatively small and the party responsible for errors is clear. Patient matching on the national scale of TEFCA is not supported by evidence and an unnecessary risk to TEFCA and the public. We urge TEFCA be built on explicit patient consent and voluntary self-identification the way that banking and other commercial networks operate.

Page 85 - ONC Request for Comment #8 - Patient identity resolution
Patient matching is a form of coercive surveillance. The introduction of data sources outside of healthcare, such as government registries or so-called “referential matching”, extends surveillance across domains unrelated to healthcare and is subject to unacceptable risks and abuses of security as well as privacy. Such practices risk having a majority of people opting out of TEFCA. The capture of all citizen data required by nations like China and Russia, forced surveillance allows government to control and harm its citizens, the opposite of Democracies that place individuals’ rights first.

Page 85 - ONC Request for Comment #9 - Patient identity resolution performance
This question highlights just how risky it is to design a national network based on untested surveillance principles. Health care is not like law enforcement where governance is well

understood and almost exclusively in the public domain. We urge ONC to abandon surveillance and patient matching as a foundation for TEFCA. Build on ethical and universal human rights to autonomy, self-determination, respect and individual consent and on voluntary self-identification as the foundation.

Page 85 - ONC Request for Comment #10 - Record location services
Record location services enable a longitudinal health record but they can also be a component of a longitudinal health record. A record locator service should be centralized or distributed among QHINs. It can also be decentralized to wherever a patient chooses to maintain a longitudinal health record. We urge TEFCA to adopt practices that do not prevent patients and innovative services that allow patients to be in control of their health record. A patient-centered independent health record can manage the authoritative list of providers, payers, apps, and other data sources that pertain to that patient.

Page 86 - ONC Request for Comment #11 - Directory services
QHINs should be required to implement standardized directory services for all public information relevant to TEFCA. This includes provider information that is already public in NPPES and Physician Compare as well as payer network participation and other information essential to decision support by patients, families, and providers. These directories should be publicly available at no cost to app and service developers. Let's keep in mind that most healthcare is either directly or indirectly paid by the Federal government and lack of consistent APIs and access to essential information is a barrier to competition where it matters most. This is the only path to enable privacy and innovation in health and health IT. Patients must be able to know and control all users of their sensitive health data.

Page 86 - ONC Request for Comment #12 - Meaningful Choice (consent) directories
The standard for communicating Meaningful Choice between directories should be Kantara User Managed Access (UMA). UMA is based on the OAuth2 standard already widely adopted by FHIR and SMART. It is a standard that allows for both institutions such as QHINs and individuals to provide authorization services, the essential component of Meaningful Choice. UMA has already been profiled by the HEART Workgroup, which is co-chaired by ONC. We recommend the adoption of UMA for TEFCA specifically because it allows for both institutional and individual (patient-centered) architectures.

Privacy-sensitive patients are reluctant to broadly share the policies by which they grant authorization with third-parties such as QHINs across the land. UMA allows patients to choose their authorization service and to keep their policies restricted to that authorization server. This creates an innovative market for QHINs to compete to provide authorization services or for patients and operate authorization services as fiduciaries. When patients don't care, UMA can still be used among QHINs by adding an authorization server entry to every patient's record locator service.

The adoption of UMA also solves a major problem, discussed in the recent ONC NPRM as the multiple portals problem, where patients are expected to monitor their Meaningful Choice policies separately across a dozens of HIPAA covered, 42CFR and non-HIPAA entities. This is clearly very hard or impossible. Again, health technology should make it easy for patients to acquire, manage, use, and enable disclosures or queries of health data. UMA provides the patient with one single point of contact that is accessed by all the other service providers to get authorization for data uses. US health technology fails unless patients have a single point of contact.

As mentioned above, building TEFCA on demographic patient matching can't succeed. We recommend the only safe and effective method based on voluntary identity linked to consent. This solves the problem of sharing demographic information as part of Meaningful Choice notices because the notices are explicitly linked to the patient identity with no additional risk or privacy burden.

Page 87 - ONC Request for Comment #13 - Meaningful Choice standards
The sharing of Meaningful Choice notices across the entire country creates an unprecedented and unnecessary privacy risk. As described above (Comment #12) a patient-controlled design for TEFCA consent management avoids the problem by keeping patient policies in a single QHIN or patient-selected service. The logging and documentation requirements for all of the other QHINs are much reduced and their liability for privacy breaches is mostly eliminated. QHINs can compete to serve as the patient's point-of-contact for Meaningful Choice and can be compensated for this additional service.

Page 87 - ONC Request for Comment #14 - Auditing
Every one of the actions listed must be subject to audit. This is the minimum for a scalable security and privacy infrastructure. The amount of information kept about each action is less important. It's reasonable to start with a minimum of information such as date-time, patient identity, data source, and authorization authority. More detailed logs should be kept by the authorization authority (sometimes called the policy decision point or the UMA authorization server). These logs can include information about the requesting party and the policy applied which, for privacy reasons, might best be kept off the network. A patient-centered and possibly patient-designated authorization service also promotes trust by offering the patient a single point of contact to audit transactions about them.

In conclusion, we are very eager for TEFCA to succeed because it can be a path to a patient-controlled independent health record that will reassure patients and restore trust in physicians, reduce errors, and lower the barrier to innovation and market entry for health services. TEFCA's path to a successful national-scale network goes through the patient.

Signed,

Adrian Gropper, MD
CTO, Patient Privacy Rights

Deborah C. Peel, MD
Founder and President, Patient Privacy Rights