CRISP

Don Rucker, M.D.
National Coordinator for Health Information Technology
Office of the National Coordinator
U.S. Department of Health and Human Services
330 C ST SW
Mary Switzer Building; Mail Stop 7033A
Washington, D.C. 20201

Re: TEFCA v 2

Dear Dr. Rucker:

CRISP is pleased to provide comments on the Trusted Exchange Framework and Common Agreement version 2 (TEFCA v 2) proposal. CRISP is a 501(c)3 HIE, governed by healthcare and government participants, which serves Maryland, D.C., and West Virginia by contract. We provide data at the point of care, push data to care managers, provide reporting and analytics for population health, support public health initiatives, and help manage several Maryland care redesign programs. CRISP has about 100 hospital participants serving a population of 8.5 million people. In a typical week, clinicians manually query CRISP at the point-of-care 90,000 times, we push bits of information directly into an EHR 700,000 times, and we send 600,000 encounter notifications to care managers. We are proud of the interoperability progress in our region.

In general, CRISP strongly supports the direction ONC is taking with regards to interoperability. We make the following suggestions.

1. **We at CRISP agree that change is needed and are generally supportive of the aims of the TEFCA v 2.** We do recognize significant shortcomings in the status quo, including these:
    a. Despite much progress in our region, significant interoperability gaps remain, especially for interoperability of records from small ambulatory practices.
    b. Within CRISP's own geography, some communities are more successful with HIE than others.
    c. Interoperability remains poor in some other states which do not have an effective HIE.
    d. Existing shared infrastructures are not directly supporting patient engagement.

    It is our observation that TEFCA shifts the strategy for moving basic health records from state HIEs to national networks. Although the shift will make certain CRISP functions obsolete, we agree with the direction. And we expect that under TEFCA, CRISP will still be able to provide value beyond basic interoperability to our participants and the patients in our region.

2. **Paired with the Data Blocking Rule, your strategy should get all providers to participate.** When TEFCA is paired with the Date Blocking Rule, it creates a strong motivation to participate in nationwide interoperability. We are feeling optimistic!

3. **ONC should support the national networks/frameworks that are currently meeting with success.** In 2016, when CommonWell announced it would become a Carequality implementer, we at CRISP saw this as the start of a nationwide solution. Since then, we have become Carequality implementers and our staff has become involved in workgroups and governance for Carequality, the eHealth Exchange, and The Sequoia Project. The Common Agreement and QHIN Technical Framework look remarkably like the Carequality framework and goals, and CommonWell, eHealth Exchange, and Care Everywhere could look like QHINs. The progress of all four continues to be impressive. While we recognize that ONC must run a procurement for the new RCE, we are concerned that if the plan does not incorporate what exists, we will all take a big backwards step, undoing the progress made in the last several years.

4. **What if requestors behave poorly? Privacy protections must be improved, perhaps during the RCE policy making process. We believe state regulations and "consent managers" could be part of the solution.** The various proposed rules seem quite focused on improving interoperability and stopping data blocking but seem to give less attention to the fact that data can be misused (e.g. seeking health information about celebrities or other national figures, snooping on family members or coworkers, etc.). Organizations which send data, which is then misused, will take little solace from TEFCA's provisions to promote exchange. Providers believe their patients will hold them responsible, not just the inappropriate requestor, for any misuse or privacy breach. We know from the examples of high-profile cases, that providers are sometimes tempted to look at data they should not. An attestation of consent on the requesting end is a weak protection, especially as interoperability makes such requests possible from everywhere.

   As an intermediary, CRISP implements certain limitations on data access based on known existing patient relationships, including a "break glass" function. We throttle the number of requests an organization can make in a single hour, to limit the damage a single breach might cause. We use third-party tools to conduct after-the-fact auditing of requests and communicate with the privacy officers of participating organizations when something looks amiss. On the order of 20,000 consumers have opted-out of CRISP, and each week we fulfill a few requests for an accounting of disclosures. With all this, we believe we need to do even more.

   By contrast, the TEFCA model only appears to address the opt-out capability (as "meaningful choice"). We believe much, much stronger protections against misuse are necessary, and we are concerned the industry could face a day of reckoning such as Facebook and the tech-titans are experiencing if we don't come up with better solutions.

   In the appendix, we have included a model which would see responders to data requests check a consent API maintained by a HIN acting as a consent management organization for a state. The very simple API request would allow for opt-out, opt-in, or granular opt-out, depending on the desires of that state. It would also form the basis for an auditing function and allow for an accounting of disclosures capability – perhaps even moving towards real-time notification of patients. We realize such a concept needs significant socialization, including with standards bodies, but are convinced that this model, or something like it, is absolutely necessary.

5. **The requirement to provide an accounting of disclosures to a patient upon request should include TPO purposes.** An accounting of disclosures is an important tool for patients to discover inappropriate use of their medical information. The fact that an inappropriate request came under the pretense of TPO should not allow the bad actor to hide that request from a patient.

CRISP responds to such requests today, and while they are made infrequently – just a few are processed each week – we expect to automate the accounting of disclosures in the future. As noted in the appendix, we believe this process can be improved in the TEFCA model through the use of state-designated consent managers.

6. **We suggest clarification that using a "jump box", in which only screen images and not data files move, does not constitute "offshoring" data.** The TEFCA contains two clauses about offshoring of data. We understand the need to limit housing of data outside the US (whether in the cloud or not), but we are concerned with the clause that indicates no disclosures or use of data can be outside of the US. Our technologists, and technologists who work for our vendors, sometimes work overseas (particularly from India). When they do, they remote into the data center with a jump box. Certain of our team members do this during visits to extended family overseas. Certain of our vendors employ some team members who live full-time in India. We would not want these rules to disrupt either activity. We ask ONC to clarify or modify the clause on disclosures and use to make it clear that the use of such jump boxes does not constitute a disclosure or use outside of the US.

Respectfully,

David Horrocks

CEO, CRISP

Appendix

State regulations and a "consent manager" to strengthen patient privacy

We see two significant problems with current approaches to protecting patient privacy.

First, based on our experience working with consumer advocates in Maryland, the current national approaches to patient privacy are not sufficient to meet patient expectations of privacy. Patients want more protection for and control of their health information. States such as Maryland have already undertaken legislative or regulatory efforts to better protect patient privacy. These efforts reflect the character and priorities of the community. Yet, at least in some instances, there is no practical way to comply with the state regulations while using the national approaches.

And, while the privacy rules are somewhat wanting, the second and more pressing problem is that national interoperability approaches have few mechanisms to monitor and prevent a participant from violating the rules. We know that clinicians who have access to records can be tempted to look at what they should not. In high profile cases we sometimes see dozens of employees caught using the local EHR to access records. As the national approaches become more successful, we will in effect give tens-of-thousands of clinicians the keys to the medical record room for the entire country. In current practice and in what is elsewhere proposed by ONC, our ability to identify misuse will be limited.

State-based HIEs usually implement additional protections. These are imperfect, but they do moderate behavior by creating the threat of being caught. Steps we take at CRISP include:

- Allowing patients to opt out so their information cannot be queried
- Checking for a known patient relationship before allowing a query, and requiring a "break glass" step if a relationship is not known
- Auditing queries after the fact using an analysis tool, and communicating with the privacy officers at healthcare organizations when something deserves more investigation
- Automatically throttling queries from particular participants, if their usage volume spikes outside of norms
- Providing patients with an accounting of disclosures upon request, so they can see who has requested their medical records from any provider in the region
- Requiring two-factor authentication for most access that does not come through a large health system (which will generally have its own two-factor authentication)

The intention in TEFCA to enable a global opt-out is a positive step, but we believe it is insufficient. And clearly, patient mediated exchange would solve some of the privacy problem. However, that requires engaged patients, and in our experience only a subset of patients will become engaged in such management. It is telling that a number of high-profile health record banking solutions have failed, although we hold out hope for Apple's recent efforts.

To improve this situation, **federal rulemaking should enable states to create additional protections and choices, using state-based HINs to manage consent and monitoring services for health information exchange**. **In this rule, compliance with the state's consent management approach should be a sub-exception to Protecting Privacy.** To enable this, rulemaking should first maintain the burden of privacy compliance on the entity responding to a query, rather than on the health information network which facilitates the query. Today, the existing national networks place the burden on the responding entity, but they do not make it easy to comply.

To make compliance easy for responding entities, states could create centralized consent databases in statewide or regional designated HINs. **The HIN would expose consent information via an API.** A responding entity would check the consent API for a consent status before responding to any data request or forwarding encounter notifications. Consent databases already exist in many states to support the state-designated HIE's own activity.

For a patient, their state's HIN would serve as a single focal point to control the exchange of their health records and to obtain information. Granular consent could be implemented if the responding entity passed information about the requestor to the consent API. For instance, at a patient's direction the HIN might allow responses to "any hospital in D.C." but treat other requests as opted out. States could make choices, including opt-in consent, and the API for that consent database would be built to respond appropriately.

The HIN would log query requests so that an accounting of disclosures could be provided to any requesting patient. The accounting could list the querying organization and responding entity for any query which was responded to in the patient's state. An HIN could also expose the log information back to patients via a push API, such that a consumer app could receive the information without the patient having to make a request. In an advanced implementation, patient consent could be requested in real time via a mobile app.

While the described approach obviously requires effort at the state level, the approach need only accommodate states which choose to designate a HIN for consent management. States which do not would be no worse off than what is currently proposed in the rule and in TEFCA. By making the logic to check a consent API prior to responding very simple and configurable, the single method could accommodate a variety of approaches.