



CENTER *for* **MEDICAL**
INTEROPERABILITY

June 17, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator
US Department of Health and Human Services
330 C Street SW
Floor 7
Washington, DC 20201

RE: Trusted Exchange Framework and Common Agreement (Draft 2)

Submitted Electronically

Dear Doctor Rucker:

Thank you for the opportunity to comment on Draft 2 of the Trusted Exchange Framework and Common Agreement as released by the Office of the National Coordinator (ONC) on April 19, 2019. The Center for Medical Interoperability (CMI) appreciates the administration's focus on achieving a more interoperable health care system, and we look forward to working with ONC as it finalizes and operationalizes these policies and proposals to advance the exchange of health information on a national scale.

The Center for Medical Interoperability (CMI) is a non-profit organization led by health systems with a mission to **accelerate the seamless exchange of information to improve health care for all**. Modeled after centralized labs from other industries, CMI serves as a cooperative research and development lab as well as a test and certification resource to address technical challenges and ensure conformance to specifications that enable comprehensive interoperability, data liquidity, and trust. Initial draft specifications have been related to medical devices within the acute episode of care.¹ CMI's CEO-level board of directors identifies health care industry technology problems that, when solved, will benefit the public good and the health care industry. CMI membership is limited to health systems, individuals, and self-insured

¹ Available at <https://medicalinteroperability.org/specifications/>

corporations, but we work with a variety of stakeholders, including medical device manufacturers, electronic health record (EHR) vendors, standards development organizations, and others, to design and engineer the technical infrastructure that will enable comprehensive interoperability, data liquidity, and the trust needed to deliver person-centered medical care.

We believe that the delivery of health care in America can be vastly improved. In an increasingly digital age where data and technology have entered nearly every facet of our lives, the delivery of health care seems relatively unchanged. In most industries, technology and data have enabled better experiences, efficiencies, and outcomes. In health care, however, it seems that technology and data have increased both complexity and costs in an already confusing and expensive system. The Center for Medical Interoperability would like to change this. By collaboratively developing an industry platform that will establish a foundation of trust between technologies in health care settings from medical devices to electronic health records, CMI envisions a world where health care data is connected, digital, accessible, trusted, secure, and useful for providers and patients alike.

The federal government has taken an active role in digitizing the American health care system through incentive payments and adjustments through programs like Promoting Interoperability. But the lack of interoperability in health care will not be solved through government action alone. It is incumbent upon the health care industry to demand better care for our patients. Data should live in the hands of patients, be under their control, and flow to and from providers to inform better treatment and care for patients. In order to achieve this, ***CMI is developing a platform to allow the trusted and secure connection of all technologies surrounding patient care.***

CMI believes that interoperability can be achieved by establishing an overarching technical architecture that supports the free flow of information on a vendor-neutral / non-proprietary platform. The technologies surrounding the delivery of health care will connect in a one-to-many, two-way, plug-and-play, standards-based and trusted manner. One-to-many means the ability to add a technology without jeopardizing others. Two-way means the ability to both send and receive data – leading to data liquidity. Plug-and-play refers to the ability to add, modify, or replace technologies without special effort on behalf of the user. Standards-based means adhering to established interface specifications. Lastly, everything on or in the platform will be trusted by conforming to technical requirements engineered to establish and maintain trust.

CMI is modeled on the belief that this platform must be driven by the purchasers and users of health technologies. ***Hospitals, health systems, and other large purchasers of health care technology and services, including HHS, should collectively align and demand that products adhere to the principles of platform architecture for data exchange.*** Benefits can be realized by all stakeholders. Right now, vendors often compete on the way that they present and process their information within their proprietary solutions. When technology vendors

align on a common platform for interoperability, it will allow them to simplify and decouple their proprietary products by leveraging the data from not only their products but from any others as needed. The innovations, efficiencies, and improvements in safety that result will benefit everyone.

Ideal State

When a person enters the office of a care provider, they should be a known entity. The health care system should recognize the person, know their complete medical history, and trust the information shared by that person. Conversely, the person should know their care provider and trust not only the ability of the provider to deliver medical care but also that the information the patient shares will be used to benefit the patient, not misused, and not shared beyond that patient's wishes.

The patient's health history should be controlled by the patient and shared with the care provider prior to the patient's visit. If the provider needs additional information, the provider should be able to obtain it from other providers, payers, or other sources with the patient's consent.

During the patient's visit, any medical devices or equipment used should seamlessly share all data generated with any other equipment that needs it and the patient's record. That record should be controlled by the patient and shared with the provider. During the visit, the caregiver can access the patient's record and use the device data to inform the appropriate steps in care orchestration and delivery. Because the patient's record is complete, the caregiver can compare trends of measurements and lab results over time and across provider organizations to better inform the course of treatment. During the visit, the patient's record is continuously updated and accessible to both the patient and the caregiver.

Following the visit, the patient can share their health information and this encounter update with other caregivers to check their opinion or better inform other courses of treatment for other conditions. With the patient in control of their data, they can take better control of their health. The patient could also choose to share their information more broadly with other entities, like researchers. With more sharing under patient control and more rich data flowing from technologies like medical devices, more robust data will be available to help inform the future of health care and the development of new treatments and cures. New technologies and algorithms could be developed to leverage this rich data to improve the practice of medicine and potentially automate some processes.

Once the technologies surrounding the patient are trusted, connected, and the data flows seamlessly, true interoperability will open the doors of innovation in ways we cannot yet imagine.

Foundations for the Ideal State

Foundational to this ideal state of health data are three principles: comprehensive interoperability, data liquidity, and trust.

By “**comprehensive interoperability**,” we mean that the technologies within an episode of care as well as across care settings and locations should be interoperable – from the medical devices used to monitor and provide therapy to patients, to the lab systems that test and diagnose, to the record system that stores and streamlines patient data for clinical use. True interoperability will come from communication across all technologies used in the delivery of health care. Typical discussions around health care interoperability center around the electronic health records systems, but these record systems are only one piece of the puzzle.

“**Data liquidity**” refers to the ability of the data to be accessed, exchanged, and used across platforms or systems without special effort or blocking from any direction. Information from one device must be useable by another to benefit the patient – otherwise the data lives in isolation and its utility is limited. Once data can flow across disparate technologies and be incorporated into each for use in the delivery of care, then the data has become truly liquid for the benefit of the patient.

“**Trust**,” as we define it, is when the information and its source are recognized and credible. The data can be relied upon by a caregiver in his or her practice of medicine as clinically valid. We also mean that the data is traceable to its source, that its integrity has been maintained through transport and while at rest and this is verifiable by the end user, and that privacy is protected. Bidirectional trust is fundamental to health care – the patient must trust the provider and vice versa. When it comes to technologies, the recipient must trust the sender and vice versa. Without trust, these relationships cease.

Connecting Technologies through a Trust Platform

To enable comprehensive interoperability, data liquidity, and trust, CMI is working with its members, technology vendors, and others across the health care industry to design and develop a platform for trust in health care. The trust platform will allow data from different technologies to flow from devices, record systems, clinical databases, data registries, and tailored applications safely and securely across the entire health care delivery system. This platform is scalable from the individual episode of care to the operations of a large health system provider. At scale, this approach would unlock previously aspirational capabilities like predictive analytics, artificial intelligence, and other models that rely on identified, contextualized, and computable data to improve care orchestration. A trust platform will be able to leverage operations tools such as the automated and secure update of medical devices to protect against cyberthreats. At the very least, connecting health care technologies through a trust platform will allow providers to focus on treating patients and practicing medicine rather than entering data, troubleshooting technology, and juggling segregated data points vital to proper treatment.

Once developed, CMI will demonstrate the utility of the trust platform through specific use cases and provide implementation specifications and guidance to scale the platform across health care systems. Acting in our role as a centralized lab, we will test, verify, and certify products, tools, and solutions to help leverage the platform's architecture in new directions as determined by the health care marketplace.

Response to TEFCA Draft 2

The proposed policies to develop a trusted exchange framework and common agreement in coordination with a recognized coordinating entity will advance the ability for health systems and providers to share patient health information if these policies are successfully implemented and sustained by appropriate resources. CMI believes that federal support for increased connectivity among health information networks and exchanges will help build a more connected and useful system and facilitate better access to necessary clinical information for use in patient care. However, CMI believes that a trust platform enabling all technologies surrounding patient care to share information in a trusted and secure way is still necessary to achieve the ideal future state of health care delivery. Further, CMI believes that ONC should lean more toward the "support" side of the statutory authority than the "develop" side considering so much work has been done in the private sector to stand up exchanges.²

Congress intended to give providers more tools to facilitate nationwide exchange when it included these provisions in the 21st Century Cures law. The intent was to provide both technical and legal language for providers who may lack the resources to establish their own exchange or join existing exchanges. Ideally, a rural provider would be able to adopt a baseline framework and a legal agreement as published by the ONC. At that point, the provider would be able to connect to existing exchanges and know the connections were technologically and legally sufficient since the documents were provided by and sanctioned by the government.

Given the larger scale of these proposals as compared to the statutory intent, CMI urges ONC to be cautious regarding the sustainability of the TEFCA Draft 2 and whether there will be adequate resources to maintain it. Recognizing the current barriers to health information exchange given the limitations of systems currently deployed, CMI believes that supporting existing exchange networks through an implementable framework and agreement for trusted exchange will help encourage information sharing while more overarching architectures are developed to enable comprehensive interoperability, data liquidity, and trust.

CMI supports the inclusion of multiple exchange modalities between qualified health information networks (QHINs). Allowing for push, pull, and search mechanisms will increase the flow of patient data and provide clinicians with more access to actionable patient information. However, CMI believes that more robust data can be shared in

² 42 U.S.C. §300jj-11(c)(9).

more ways through industry adoption and implementation of a scaled trust platform that would allow connection between all technologies surrounding patient care and not just certified EHR products.

CMI supports ONC's decision to limit the initial requirements of the common agreement in order to ensure the success and scalability of the proposal. CMI also believes that a phased approach is wise to build momentum and support across the health care industry and allow for more widespread adoption and participation. Simultaneously, it is important that ONC is taking an approach that would "not limit the ability of HINs to innovate and build additional services."³ While it is important to set baseline standards to encourage industry-wide adoption and use of the trusted exchange framework and common agreement, it is also important to allow room for the private market to innovate and expand beyond those baselines.

CMI applauds ONC's proposal to require non-HIPAA entities to be "bound by certain provisions that align with safeguards of the HIPAA Rules."⁴ CMI believes that trust is foundational to the success of interoperability and HHS should encourage elements that support trust, privacy, and security as it implements these proposals. To that end, CMI encourages ONC to work with the Office for Civil Rights and other offices and agencies at HHS and in other departments of the federal government to ensure that privacy and security requirements related to the exchange of health information are adhered to and enforced across jurisdictions. CMI will continue to develop the trust platform as a mechanism to enable trust between technologies surrounding patient care, including the ability of those modalities to exchange with entities not traditionally engaged in health care delivery.

CMI believes that "meaningful choice" is a good first step in allowing patients to have more insight and control over the uses and disclosures of their own protected health information. CMI encourages ONC to consider the possibilities of tagging metadata to allow for traceability so that patients can follow the actual uses and disclosures of their information and access audit trails of the data as it leaves their provider, personal electronic device, or their personal longitudinal health record. This would increase the ability of patients to understand how their health data is accessed and used. CMI envisions a future where patients control the access and use of their health information.

Principles for Trusted Exchange

Standardization

CMI agrees that health information networks should adhere to applicable standards adopted by HHS to ensure conformity across the industry and enable the exchange of

³ The Office of the National Coordinator for Health Information Technology, [The Trusted Exchange Framework and Common Agreement \(TEFCA\) Draft 2](https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf) (April 19, 2019), p. 15, available at <https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf>

⁴ *Id.*

health information between disparate systems. CMI believes that technology should be implemented in easy-to-use ways, but CMI also cautions that the source technologies themselves should have room to innovate and not just the connecting technologies.

Transparency

CMI also agrees that transparency will help enable better understanding of information exchange for patients and providers alike. CMI urges a balance between the desire to allow patients unfettered access to their own health information and the need for health information networks, providers, and others engaged in care delivery to educate patients against potentially unwanted uses and disclosures of such health information. CMI believes that trust is necessary across all the transactions considered in these proposals, but especially when health information leaves traditional pathways where it is regulated by health care privacy and security laws.

As consumers have become more aware of how technology companies are using their information, more public scrutiny and even outrage has started to permeate. Congressional committees are currently discussing how to respond to these consumer privacy concerns and news outlets such as *The New York Times* have dedicated projects to privacy as a national issue. A recent study in the *Journal of the American Medical Association* found that nearly every application for depression or smoking cessation shared data with third party services provided by Facebook or Google, but only a few of them correctly disclosed this fact in their privacy policies.⁵

CMI believes it is incumbent upon the private sector to get ahead of this conundrum by developing and deploying a trust platform architecture and governance structure on behalf of its health system members. CMI also believes it is in the best interests of app developers to actively engage in this discussion at the outset. If appropriate consideration is taken to generate a solution that fosters both data exchange and trust simultaneously, both the developer economy and traditional health care economy win, not to mention patients. CMI stands ready to work with its members and others inside and outside of health care to advance interoperability, patient access, and trust among all parties and associated technologies.

Cooperation and Non-Discrimination

CMI supports the discouragement of practices that may inhibit the access, exchange, or use of health information.

Privacy, Security, and Safety

⁵ Kit Huckvale, John Torous, Mark Larsen, [Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation](https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=twitter&utm_campaign=content-shareicons&utm_content=article_engagement&utm_medium=social&utm_term=042219), *JAMA Netw Open* (April 19, 2019), available at https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=twitter&utm_campaign=content-shareicons&utm_content=article_engagement&utm_medium=social&utm_term=042219.

CMI believes that the use of unique patient identifiers that can be leveraged by patients and participating private health care providers can enable timely and accurate sharing of data, easier consent management, and the creation of personalized care strategies based on complete data sets. ***Investment in and industry adoption of a trust platform, supported by an appropriate governance model, based on a distributed architecture with strong identity protocols could pave the way for a simplified patient identifier for use in health care delivery.***

While CMI believes that a secure identity solution will be superior to matching, we support efforts to improve patient matching in the interim. Focusing on data quality at the point of collection and alignment around common data elements for demographics would be helpful.

CMI also believes that trusted data re-entry is vital to a functioning system of health information exchange and therefore supports the use of standard nomenclatures and structures to allow the recipient to readily consume and use the information in clinical care.

Patient consent and control over the uses and disclosures of their own health information is key to securing the patient's trust in the health delivery system. CMI supports the notion that the framework should "engender trust amongst other entities seeking to exchange with that network."⁶

Access

CMI believes that adherence to data sharing agreements is necessary to enable an environment for trusted exchange. We caution ONC and HHS overall to carefully consider the potential ramifications of protected health information leaving the regulatory regimes surrounding traditional uses and disclosures of health information. Patients should have opportunities to review and reject policies that may go beyond that patient's desired level of use or disclosure. Additionally, a robust system of health data exchange should allow patients to revoke consent and track the uses and disclosures of their data wherever it may flow.

Population-Level Data

CMI supports the proposed "bulk transfer" capabilities envisioned by these proposals for use in population health management and overall improvement of the health care industry. CMI agrees that robust privacy and security standards are necessary before these types of transfers can take place.

Qualified Health Information Network Technical Framework (QTF)

CMI has reviewed the technical framework and is supportive of the overall methodology. The emphasis on foundational security elements, such as identity, authentication, digital

⁶ Office of the National Coordinator, *supra* at p. 28.

signatures, encryption, auditing, and error reporting, aligns well with CMI's architectural approach for interoperability, data liquidity, and trust. We recommend the recognized coordinating entity (RCE) explore mechanisms for cross-domain authentication for seamless and secure data communications across solution domains that leverage different Certificate Authority and Public Key Infrastructure solutions. This will facilitate compatibility across QHINs as the RCE builds out digital identities.

To further facilitate interoperability between QHINs, CMI recommends that the RCE specify a standard format for identifiers, record location services, transaction reporting, and error reporting. We highly recommend that these formats be extensible for future enhancements within the trusted exchange framework to allow QHINs to offer richer data services to their participants as the framework evolves.

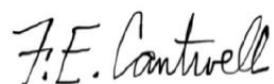
We recommend that the RCE take an iterative approach in coordination with QHINs to normalizing directory services, patient identity resolution mechanisms, meaningful choice communication, and consent. We recommend that these chosen solutions also allow for extensibility for future enhancements.

As an additional comment on the technical requirements, we recommend that the QTF include a mechanism, such as Network Time Protocol, to enable time synchronization across QHINs so that queries, responses, and transaction logs can be properly correlated in time.

Lastly, CMI notes that the ONC has posed several questions regarding technical details pertinent to the design and operation of the framework. As this type of detail is best considered through an iterative design process, we recommend that the chosen RCE convene a technical working group of relevant industry participants to address questions and assist the RCE in its ongoing role to develop, update, implement, and maintain the QTF. CMI stands ready to participate in such a working group or to assist the RCE in other ways in support of trust and interoperability.

Sincerely,

Center for Medical Interoperability

A handwritten signature in black ink that reads "F.E. Cantwell". The signature is written in a cursive style with a large, prominent initial "F".

Ed Cantwell, President and CEO
8 City Blvd., Ste. 203
Nashville, TN 37209
info@center4mi.org
(615) 257-6400