June 17, 2019

Don Rucker, M.D.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Resources
330 C St SW, Floor 7
Washington, DC 20201

Dear Dr. Rucker:

On behalf of the DirectTrust community, thank you for the opportunity to submit comments in response to the Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2.

Who We Are

The Direct Standard™ is a federal standard for interoperable electronic health information exchange, embedded in over 400 Certified Electronic Health Record Technologies, whose end users can send and receive Direct messages and attachments.

The Direct Standard was developed to enable a simple, safe, secure, and interoperable way to send and receive patient data between providers using different EHR systems in different institutions over the Internet. Direct exchange is now available to over 1.8 million clinical end-points and 265,000 patients/consumers in over 167,000 health care organizations in the United States.

In 2013 a cooperative agreement was awarded to DirectTrust by the US Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC) to participate in the Exemplar HIE Governance Program. Since that time, DirectTrust's Trust Framework has evolved to become a dynamic and voluntary technical and human system, involving legal, policy, infrastructural and governance components. The primary purpose of the Trust Framework is to instill confidence in the security and identity controls all parties apply to their roles in exchange. The Trust Framework "scales" trust by making it unnecessary for relying parties to negotiate one-off agreements for trust. It creates a "network of trust."

At the heart of DirectTrust's Trust Framework is its Public Key Infrastructure (PKI) for identity credentialing and access management. DirectTrust has been working closely with various health IT stakeholders to test new ways of leveraging components of its governance and technology to support the security and scalability of FHIR-based API access to electronic health information (EHI).

Summary Comments

DirectTrust applauds the goals of the Trusted Exchange Framework Draft 2 to advance nationwide healthcare interoperability and establish a "single on-ramp" embodied by the notion of a Common Agreement, which would enable organizations to connect to all of the participants in the TEFCA system to access and use all available electronic health information (EHI).

However, if the Common Agreement is to effectively support these goals, the framework for participation needs to be flexible enough to involve a broad array of stakeholders and support exchange by all current and future interoperability elements and standards, without adding additional complexity or costs to the existing systems for exchange. In the absence of such flexibility, the Common Agreement risks becoming irrelevant as the healthcare information technology landscape continues to evolve through powerful market forces interacting with government regulations and programs. The framework needs to be able to better take advantage of the players and assets already in place – particularly with regard to the standards cited for "push" messaging. Also, it will need to support appropriate governance and controls for the technological approaches to exchange that are emerging now and may emerge in the future. We strongly advocate for TEFCA and the final QHIN Technical Framework (QTF) to be consistent with the approach in ONC's 21st Century Cures proposed rule, with regard to support both for all current interoperability elements and for FHIR and the new app economy to make the policy direction clear for all stakeholders.

The first version of the Trusted Exchange Framework was released in January 2018, as the national query exchange frameworks (CommonWell, Carequality and SHIEC's Patient Centered Data Home) just began to demonstrate traction. The first version dealt almost exclusively with support for the query of a patient's records wherever they sought care utilizing available standards. As such, TEFCA Draft 1 was relatively prescriptive in terms of technology to allow for nationwide scale for patient discovery and record-location. Our understanding is that the notion of a QHIN came from a perceived need to create nodes on a network of networks where a relatively small number of players would be able to interoperate to find where the patient had been and to assemble all of their records.

TEFCA Draft 2 has altered the approach in several ways. First, it allows existing entities supporting health information exchange to connect through QHINs to other such entities and to connected Participants and Participant Members. This may have a positive effect of making good use of existing exchange entities HIEs and their current participants as they are deployed regionally today. Also, TEF eliminated specific requirements for QHINs that would prescribe mechanisms for end-point and patient discovery opening the door to alternative approaches to satisfying the functional requirements of query-based exchange and qualifying more organizations as potential QHINs. Another significant change was to eliminate population health queries in response to comments that such capabilities were immature and to introduce

instead "QHIN Message Delivery" acknowledging the value of "push" messaging for care-coordination and for public health.

The players and pathways prescribed in the new version of the Trusted Exchange Framework and the draft QHIN Technical Framework leverage many of the existing mechanisms and stakeholders for query exchange but make no use of the considerable investments made by government and the industry in the DirectTrust Network. Direct messaging and the players that enable it are an extremely valuable asset that has been ignored by TEF, favoring instead a push messaging replacement utilizing a different topology and a lesser used standard, the IHE XCDR. This is a missed opportunity, because the DirectTrust nationwide network has already achieved the high-level goals of both 21st Century Cures and the TEF, and could be leveraged to accelerate progress on innovative use-cases that have not yet been fully addressed by alternative mechanisms.

The goals of the Trusted Exchange Framework are laudable and expansive. At a high level, the TEF's goals are to:

- "*Provide a single "on-ramp" to nationwide connectivity*"
- "*Enable Electronic Health Information to securely follow the patient when and where it is needed*" and
- "*Support nationwide scalability*"

These goals are consistent with the substantial achievements made by those at ONC and in private industry who worked over the last 8 years to enable national interoperable exchange via the DirectTrust network. We urge ONC to build on what is already working in the market, rather than redirecting to older, out-of-date standards or incentivizing replication of exchange mechanisms, such as Direct messaging, that are working well for stakeholders today.

The DirectTrust community urges ONC to focus its efforts and resources toward supporting the relatively few national trust frameworks already functioning across the nation. We recommend a more lightweight approach, consistent with the legislative mandate set out in the 21st Century Cures Act, directed at establishing the *minimum* conditions for efficient trusted exchange to occur.[1] We encourage ONC to build on what's working, rather than creating an entirely new construct with significant complexities and the potential for increased costs, given that simplified exchange mechanisms are already functional today. Layering a QHIN-Participant-Participant Member structure onto this functionality adds complexity and potential cost with little added benefit, and a multi-layered structured may disrupt services that are working well for providers and patients today.

[1] 130 STAT. 1166. "The common agreement may include… organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur…"

Given ONC's goal of increasing interoperability between existing networks, which we believe is a laudable one, DirectTrust advocates for a more initially minimal approach, such as focusing on individual access and treatment purpose in the short term (e.g. years 1 and 2) and evaluating progress and troubleshooting issues before implementing additional Exchange Purposes in subsequent years. This more agile and iterative approach would more appropriately tie back to the goals of Congress in 21st Century Cures, including ensuring that electronic health information will "follow the patient" for the most basic purposes – individual treatment and access – that all stakeholders can agree upon.

Other purposes, such as the ability for QHINs to query for business and management purposes – e.g. their own commercialization of competing products – may prove to be more controversial and erode patient trust in the system.

We propose that ONC allow and encourage existing frameworks to operate cooperatively to create a Common Agreement that is truly focused on the minimum conditions for efficient trusted exchange, or alternatively, to allow and encourage the RCE to create more formal coalitions of these same players to achieve the same goals without limiting or prescribing what roles such stakeholders are allowed to play. Either approach could enhance the goals of TEFCA and take best advantage of our collective assets without upending the market for healthcare exchange fundamentally.

SPECIFIC COMMENTS AND RECOMMENDATIONS ON TEFCA

1. **Modify the definition of a QHIN in TEF to allow broader participation**
2. **Enable and Encourage Care Coordination and Referrals**
3. **Reduce the risk of consolidation in a diverse community of competitive players**
4. **Ensure the RCE will Collaborate with Stakeholders Through Appropriate Oversight**
5. **Support Secure Messaging by Patients as an alternative to FHIR for Individual Access**
6. **Recognize the Importance of Governance and a Technical Trust Framework for FHIR**
7. **Promote the use of the Direct Secure Messaging in Public Health**
8. **Leverage Identify Proofing at Existing Networks and adopt standard Certificate Policies**
9. **Without changes, TEFCA participation should not provide a Safe Harbor**

1. Modify the definition of a QHIN in TEF to allow broader participation

Under our federated services agreement, the 37 HISPs of the DirectTrust Network already enable connectivity between more than 167,000 health care organizations served by over 400 different electronic health record systems. With just a single agreement, or even as a part of the contract for their EHR system, each of the 1.9+ million connected parties can exchange messages securely with each other needing only to know the other party's Direct address. Users don't need to know what technology supports them or what gateway they are behind – the connectivity is seamless and has demonstrated success around the country.

Since DirectTrust qualifies neither as a potential RCE (as we are also a HIN and so prohibited) nor as a QHIN (since we don't enable all required modalities) the value of our assets to the challenges the TEF seeks to address are lost to the new framework. As Participants, all our traffic would be expected to be through the QHIN which is inconsistent with the way the protocol works and would require every existing contract for HISP services to be rewritten and likely result in market consolidation. *In conversations with numerous ONC representatives over the past year, the message has been consistent that Direct messaging was expected to be outside of TEFCA by design.*

While we don't believe we need to be inside TEFCA for Direct messaging to work, we do believe that as we move toward an app economy and FHIR connectivity DirectTrust can make a significant contribution by providing the governance framework for secure, scalable technical trust. We also believe that introducing an alternative to Direct messaging that QHINs are obliged to offer represents unnecessary effort, costs and risks.

Recommendation: ONC should explicitly encourage the use of DirectTrust and other successful networks already in place, rather than stand up an inconsistent, alternative for push messaging within the QHINs. QHIN message delivery will require replication of both governance and infrastructure of the sort DirectTrust already has in use at scale. The TEFCA structure must be flexible enough to support and/or interoperate with existing exchange frameworks that are the result of significant public and private investment and resources. In keeping with the decision to separate the QTF from the Framework, incorporating it by reference, ONC should leave the precise role and obligations of the QHIN to the RCE in collaboration with all stakeholders and remove it from TEF. DirectTrust looks forward to the opportunity to collaborate with the chosen RCE to make the best use of our assets in the service of nationwide healthcare data exchange.

2. Enable and Encourage Care Coordination and Referrals

Under the 2015 Edition of the Certification Program, certified health IT systems are already required to be able to send and receive Transitions of Care (ToC) information through Direct

messaging. In Q1 of 2019, over 164 million Direct messages were sent and received in the network, most of which represent the ToC use case. Transaction volume has continued to rapidly increase – our Q1 volume represents a 49% increase over the same time last year.

Direct messaging represents the only currently available, widely implemented, standards-based approach to electronic referrals in the market and advancing this capability to better support closed-loop referrals and active care coordination is the logical extension of the transitions of care requirement. Stakeholders in collaboration with the ONC are currently engaging in standards development work to solidify this workflow, utilizing 360x[2] over the DirectTrust Network. Direct messaging also remains the most cost-effective mechanism to connect care providers with either uncertified EHR systems or those with no such system, particularly in the post-acute realm because of the extremely low comparative cost of onboarding these endpoints – they need only to get access to a Direct address. This allows for health records to follow the patient to places where interoperability through other mechanisms is rare because of economic realities, like rehabilitation centers, home-care and hospice. The HISPs of the DirectTrust network are making these connections at scale today connecting these locations to the all other players on the network.

Recommendation: As a part of the flexibility that could be afforded the RCE under a less prescriptive TEF, ONC should encourage the adoption of existing and emerging capabilities to support active care coordination through closed-loop referrals. In further rule-making, ONC should provide incentives and direction to the health IT development community by incorporating support for such workflows in the Certification Program. ONC should encourage participation in Direct messaging for the post-acute space as a primary means of connectivity.

3. Reduce the risk of consolidation in a diverse community of competitive players

Competition in the health IT market has positive effects. However, the impact of TEFCA as currently proposed may be to increase consolidation in the market among a set of limited QHINs which are subject to stringent requirements that may pose a barrier to entry for other players. A strategy of consolidating power and authority in the hands of a few entities may have certain unintended consequences and risks. There is a particular risk in having a single entity, the RCE, maintain control over key policies and agreements that will influence the activities of an entire industry. Additional risks could include the exit of innovative players who do not want to comply with the complex requirements on QHINs/Participants/Participant Members; the abandonment of existing frameworks and networks that are already working well today; and the

[2] 360x Implementation Guide
https://oncprojectracking.healthit.gov/wiki/display/TechLab360X/360X+Implementation+Guide

addition of new layers of complexity and cost inherent in a four-tiered system on top of existing exchange mechanisms.

Ideally, TEFCA would "*promote(s) innovation and competition at all levels*" while also supporting the goal to "*build on existing trust frameworks, infrastructure and capabilities*" that is essential if momentum toward success is to be realized and sustained. Providers must have access to EHI "*regardless of what health IT developer an organization uses" or "how far across the country an individual's records are located.*"

The DirectTrust Network already supports these goals – our community of network operators - the accredited Health Information Service Providers (HISPS), the Registration Authorities (RAs) and Certificate Authorities (CAs) of our community actively compete with each other as they work to create seamless integration and better user experience with EHR systems. Some health IT developers provide these capabilities themselves and operate nodes on our network by becoming HISPs and/or RA/CAs. With every certified health IT system already offering these existing capabilities, and providers across the country already having invested time and resources in implementing and training staff to use them, it seems a duplicative waste of resources to deploy a secondary, parallel system for push communication.

Recommendation: ONC should not risk encouraging further consolidation in an existing competitive market that might be brought about by requiring QHINs to offer an entirely different approach to push messaging than is already supplied by a large group of independent players. Instead, ONC should consider the HISP market as a working baseline to allow for cost-effective onboarding of exchange participants that use hundreds of different technologies offered by small and specialty focused companies or that use an entirely different set of productivity tools such as is found in public health or at payers.

4. Ensure the RCE will Collaborate with Stakeholders Through Appropriate Oversight

The RCE will have significant power to add terms and conditions to the Common Agreement and set technical and functional requirements for QHINs and other entities participating in TEFCA. Currently, ONC has oversight over many key aspects of the RCE's activities. However, DirectTrust advocates for a more diverse governance board, including participation from various impacted stakeholders, to supply additional necessary checks and balances to the RCE's activities. This will ensure that stakeholders are heard and have an impact on the direction of these policies, as not all of the policies will be subject to the regulatory notice-and-comment process.

Recommendation: ONC should carefully consider the powers and authority of the Recognized Coordinating Entity (RCE) and establish an adequate oversight and public input process that is transparent and fair to all impacted stakeholders.

5. Support Secure Messaging by Patients as an alternative to FHIR for Individual Access

DirectTrust is and has been committed to achieving the goals set out in TEFCA and in the Information Blocking rule. DirectTrust naturally supports the goal to "*empower(s) individuals to use their Electronic Health Information to the fullest extent*" and to "*enable(s) providers and communities to deliver smarter, safer, and more efficient care*." Our Consumer Patient Participation Workgroup and our broader community has been working to lay the groundwork for electronic communication between patients and providers without the need to have an existing relationship with the provider or credentials in their portal. In order to support self-referral and interactive communication, Direct Secure Messaging provides a unique capability to enable such a value proposition. The Secure Messaging requirement (which the latest notice of proposed rulemaking has removed from the certification rule) was in support of this initiative and as we offered in our comments to the rule we believe it should remain a requirement, in addition to new requirements for patient's to get access to their own records utilizing APIs and an "app of their choosing".

We are aware of the issues that have made secure messaging between consumers and providers less successful that it might have been. To address these, we are embarking on new programs to help provider organizations implement appropriate processes to ensure the right personnel are engaged in such communications so as not to increase provider burden. In support of this, the DirectTrust aggregated directory has added a field in our latest version that indicates whether the address can be seen by patient/consumers or only by providers, with the goal of allowing the flow of messages initially only to the appropriate resources in the practice or hospital. We also are working to implement extensions to standards and develop new standards (See "Leverage the Identity Proofing Capabilities of our Network" below) that would allow for new communications capabilities and for the digital signing of data released to patients to ensure that when the data is forwarded to another provider the context and integrity of the data as curated by the provider is maintained.

Recommendation: For the individual access modality, TEF should allow and encourage existing mechanisms for consumer participation in the exchange of their records through Direct messaging. Likewise, the ONC should collaborate with the DirectTrust community to better educate providers on the value of such communication vehicles and ways to make them less burdensome.

6. Recognize the Importance of Governance and a Technical Trust Framework for FHIR

While APIs hold great promise as an approach for query-based EHI exchange, industry still lacks a nationwide trust framework for the third-party applications that will be facilitating patient access to EHI or as these same APIs are utilized for exchange amongst covered entities and business associates. TEFCA does not address these requirements fully as it remains focused on current exchange approaches through the IHE profiles.

The DirectTrust Network is a model for how numerous endpoints can be quickly and easily on-boarded in a certificate-bound, directory-based model that simultaneously ensures security and trust. Analogous requirements for identity proofing, directory management and security will be needed in a future where APIs and other protocols are used for push messaging and server-to-server integration. The identity proofing activities which are done for Direct messaging purposes could be leveraged for other technical endpoints and for other purposes at the same facilities.

DirectTrust also operates a directory aggregation service that collects direct addresses from all participating organizations that will share them and allows the aggregated set to be downloaded for access from within the workflow of electronic health records systems. This unique federated approach allows for onboarding of new discoverable endpoints without effort allowing for scalability and reach that is unrivaled in the industry.

In the emerging app ecosystem, DirectTrust's existing trust framework could be leveraged to certify that appropriate security safeguards are in place for these applications including auditing authentication and identity proofing processes and mechanisms to ensure "meaningful choice." By certifying or accrediting processes and binding the applications to a digital certificate governed by trust policies, applications could be vetted once and universally trusted to dynamically register and connect to APIs at any endpoint. This would also allow the revocation of these certificates in the case of non-compliance with applicable standards or if application developers are otherwise identified as "bad actors." In the future as APIs begin to support database "writes" or the equivalent to push messaging through FHIR or other protocols, the same sort of identity proofing requirements and directory management that support the security and scalability of the DirectTrust network will become essential to ensure the integrity of a patient's health record.

Recommendation: ONC and/or the RCE should collaborate with DirectTrust and the Direct community to adapt the DirectTrust model for use with the FHIR ecosystem as a component of a more complete fabric for health information exchange.

7. Promote the use of the Direct Secure Messaging in Public Health

TEFCA Draft 1 made no mention of or accommodation for the public health sector as this draft focused attention on query-based exchange for treatment purposes almost exclusively. According to TEFCA Draft 2 and of the published deliberations of the TEFCA Taskforce, the introduction of XCDR based push messaging in TEFCA Draft 2 is specifically to address the needs of public health. Ironically, the current Direct messaging ecosystem supports Direct XDR which is a protocol which allows edge systems to take advantage of the scalable end-point discovery and security capabilities of the Direct Standard while utilizing the legacy profile called for in TEFCA Draft 2.

There are substantial demonstrable uses of the DirectTrust Network for public health today both at the state and federal level. These have shown extraordinary growth in only the past 12 months. As an example, the Massachusetts Health Information HIWay[3] or Mass HiWay launched in October 2012 and exercised a strategy based exclusively on Direct Secure Messaging for transport. Over 90% of the traffic on the HIWay is bound for the state public health department and this represents the sole mechanism to communicate the tens of millions of transactions that are sent to the state. At the federal level, The Centers for Disease Control and Prevention deployed the National Healthcare Safety Network[4]. The CDC contracted with a DirectTrust accredited HISP to support the acceptance of C-CDAs through a process referred to as Direct C-CDA Automation.

The HISP network operators that serve public health end-points are seeing exponential growth in traffic in just the past year – for these players, public health transactions represent the majority of their messages received. That said, as communication of data of this type over the DirectTrust network is better understood by the provider community, each of which is connected to Direct through their accredited HISP, all HISPs will see public health traffic outbound from the EHR systems as demand for and deployment of this low-cost mechanism for interoperability increases.

The most significant barrier to success utilizing Direct for public health (and for that matter, for an effective replacement for fax communication with payers) is not that standards for communication are lacking or that a trust framework is absent. *Rather the issue is the lack of standardized capabilities in the EHR market for this use-case.* All certified health IT systems support the communication of Transitions of Care and referrals, and likewise, nearly all of these systems also support the attachment of documents other than Consolidated CDA documents. Most can include XDR packages as Direct message attachments containing both structured and non-structured data. *Some, but not nearly all, also provide a mechanism to send messages containing documents of any type on one or more than one patient which would support the public health use case today.*

The greatest barrier to this use case is the reluctance of the EHR systems to offer connectivity through the Direct messaging channel as an alternative to individually orchestrated and sold point-to-point interfaces already developed since these provide both services and licensing revenue for them. Before the ubiquitous availability of Direct messaging, HISPs provided effective work-arounds for this issue by offering services to accommodate a variety of mechanisms from practices, turning messages of any type and any transport mechanism into Direct messages and forwarding them to the appropriate end-point. While this has represented an opportunity for our individual members, they universally agree that the overall ecosystem

[3] The Massachusetts Health Information HIWay http://www.masshiway.net/HPP/index.htm
[4] NHSN CDA Submission Support Portal (CSCP) https://www.cdc.gov/nhsn/cdaportal/importingdata.html

and society is better served by making the most of the positive network effects of a more open "in-door" from the EHR to Direct Secure Messaging.

Recommendation: Rather than offer an alternative mechanism for push messaging to serve the Public health sector, ONC and the RCE should collaborate with the Direct messaging community to make the most of current capabilities in the market to connect public health and payers. In further rulemaking, ONC should add requirements for push messaging for this use case to the Certification Rule.

8. Leverage Identify Proofing at Existing Networks and adopt standard Certificate Policies

DirectTrust has invested resources and time into leveraging aspects of our technologies and governance in new contexts, and particularly to grow our identity proofing capabilities. We urge ONC to focus on supporting efforts such as these, which would make significant progress toward the goals of TEFCA.

For example, DirectTrust Registration Authorities identity proof individual providers and patients as well as organizations and departments within those organizations. This process leverages the scale of the healthcare market itself by accepting the veracity of assertions by provider organizations and others (under appropriate contractual terms) that hire and credential providers and/or deploy technical infrastructure. Each of these endpoints (and sometimes individuals) is bound to a digital certificate that is used today for the purposes of securing both transport of messages and near-real-time communication via Direct Secure Messaging. While this process is fairly lightweight, the rigor, effort and cost associated with it could be leveraged for other purposes.

For example, as an organizational identity proofing event is conducted for the purposes of issuing a Direct address and a digital certificate, the same event could be leveraged to issue certificates for query-based exchange. Query exchange end-points today are issued in a variety of approaches and under different certificate policies which makes it difficult to identify the set of end-points that serves a given healthcare organization or to establish universal trust. Associating these activities and imposing the same governance requirements and certificate policies on all participants in exchange could improve security and interoperability while producing an authoritative source for a comprehensive directory of healthcare endpoints across the nation.

In terms of individual identities, the DirectTrust network is the only nationwide exchange framework today that has certificates bound to individuals. The individual Direct addresses and their association with organizational domains has value in a variety of ways. First, being able to navigate to a query location (whether this is a FHIR end-point or an IHE gateway) having received a Direct message requires the ability to create the cross-walk between individuals, the organizations they are a part of and the gateway end-points behind which their data resides.

The complexities of the many-to-many nature of this healthcare hierarchy are best captured and maintained by a process that is operationally authoritative and operated under transparent governance.

Once an individual provider has been identity proofed, a certificate can be used to digitally sign data when such data is shared with patients or others allowing recipients to know that it has not been altered even in cases where the data has been forwarded to other parties. Standardizing certificate policies and including this capability as a part of supported, if not required, capabilities for exchange participants can further harden the ecosystem preventing willful misrepresentation of data about patients.

Identity proofed FHIR clients can also take advantage of this capability as described above to allow them to dynamically register with FHIR end-points saving costs, time and promoting scalability of the ecosystem.

Our organization has also been collaborating with other stakeholders to allow for identity proofing events to be scalable across enterprises, e.g. "scalable trust." This could be used to support for a common sign-on that could function across organizations that are a part of this framework for providers and even consumers – reducing one of the major friction points for users.

DirectTrust is also actively working to build out the ecosystem for improved scalable identity proofing consistent with NIST 800-63-3 by collaborating with technology companies that leverage Real IDs and cell phone workflows to identity proof consumers at scale augmenting registration authority processes. Likewise, in terms of validating identity claims made by individuals we are pursuing connectivity with authoritative data sources to validate identity evidence. This includes the APIs that are made available by both the American Association of Motor Vehicle Administrators (AAMVA) to validate the data on Real IDs and the Federation of State Medical Boards (FSMB) to validate both provider identity and asserted credentials.

Recommendation: To realize the goals of TEFCA on the ground, ONC should encourage the RCE to collaborate with organizations like DirectTrust that are working to identity proof the healthcare ecosystem at scale. This can provide a foundation for scalable trust that allows for the individuals and organizations to proof once and leverage this event for multiple purposes.

9. Without changes, TEFCA participation should not provide a Safe Harbor

Our membership does not believe that the TEFCA in its current form offers an appropriate safe harbor from penalties associated with the information blocking rule. As we shared in our Comments to the NPRM, TEFCA as proposed covers only a portion of the interoperability

elements, standards and purposes in use in the market today. We propose that real world testing and on-the-ground data collection offers a better opportunity to truly understand whether users can actually send, receive, find, and use EHI.

As it stands today, TEFCA is laying the groundwork for what could potentially lead to discriminatory practices that favor communication mechanisms that go through a relatively small number of QHINs rather than through mechanisms that will, based upon the current definition, need to be outside of TEFCA. This includes the broadly deployed network capabilities of the DirectTrust network and new FHIR based approaches that will emerge.

Offering a safe harbor will provide an overwhelming incentive for participation in TEFCA to limit liabilities, but will also provide cover for any behavior not explicitly defined as unlawful in the MRTCs or ARTCs. This will effectively gut the efficacy of the much-needed information blocking rule. Further, important issues that are covered in the information blocking rule, such as access to interoperability elements and the seven exceptions, would not be fully addressed through participation in TEFCA.

Recommendation: TEFCA Draft 2 is not an adequate safe harbor for compliance with the 21st Century Cures Act's legal prohibition against information blocking. ONC's proposed regulations on information blocking are critical to making interoperability elements that are hidden or difficult to use more transparent and accessible. Instead of a TEFCA-based safe harbor, DirectTrust advocates that ONC incentivize health IT developers to demonstrate interoperability with real-world testing, and show that appropriate users can locate and operate workflows like Direct messaging on the ground.

Conclusion

DirectTrust and its members stand ready to work with ONC, the RCE, and all health IT stakeholders to implement the goals of 21st Century Cures. We believe these goals will be best served by a more agile, incremental approach implemented through pilot testing with full transparency and stakeholder input.

Respectfully,
Scott Stuewe

President and CEO
DirectTrust