September 23, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology

Attention: ISA Comments

Dear Dr. Rucker:

On behalf of iShare Medical, we applaud the ONC for its determination to find a solution to the complex problem of trust in healthcare interoperability. We agree with the ONC that the use of common standards advances interoperability.

The following comments are on behalf of iShare Medical in response to:

Background

We believe that there has been significant changes in HealthIT and that standards evolve including:

- The advancement of FHIR and the call by CMS and ONC to develop FHIR API's
- Leveraging of DirectTrust Framework for transport of FHIR Messages to provide a bridge from where we are today e.g. DirectTrust Direct Messaging to the future FHIR API's
- Use of Certificates to digitally sign Jason Web Tokens (JWT) in real time thus allowing trust to be established in real time and creating scalable FHIR transactions

We believe that these advances in regulations, approach, and technology should be incorporated in the standards.

PUSH Exchange

We disagree with the removal Direct Secure messaging from the 2015 Edition. Non-profit DirectTrust is the ANSI Accredited Standards Development Organization for Direct Secure Messaging. Further, we are concerned that the ONC may be under estimating how much Direct Messaging is being used in the backend of systems to power HL7 V2 ADT messaging, transitions of care, referral management, prior authorization for services, reporting to Registries and Federal Agencies, and support for CPC+.

In order to move forward, we need to build a path from the present to the future. We agree that FHIR is the next generation of interoperability; however, FHIR is not widely adopted today. EHR's are adding FHIR capabilities to their EHR's but this is a lengthy process. Only three of the top ten EHR's have more than single digit adoption rates of version 2.0 of FHIR (the current release of FHIR is version 4.0.0). The FHIR standard is moving quickly and will become the next standard, but please give the industry time to implement this standard.

Direct Secure Messaging; on the other hand, is the most widely adopted interoperability solution deployed today. Direct Secure Message is a part of every Certified EHR system which makes Direct Messaging the fastest way to deploy wide-spread interoperability.

DirectTrust Direct Secure messaging widely adopted and powering interoperability. DirectTrust has been experiencing exponential growth bringing nationwide interoperability to reality. DirectTrust reported first quarter 2019 results: 1.9 million DirectTrust Direct Addresses from 167k healthcare organization transacting 164 million transactions per quarter (55 million transactions monthly). Carequality, in contrast, reported per its website: 600k providers from 40k clinics and 1,400 hospitals. This comment is provided only as a reference to the volume of another organization and is not provided for any other purpose.

The non-profit DirectTrust is the largest health information exchange network in the U.S. and includes a diverse group of stakeholders as DirectTrust Accredited Trust Anchors and members who use the DirectTrust Direct standard for interoperability. DirectTrust's diverse members include, but are not limited to: insurers Anthem and UnitedHealthcare Group, EHR vendors Cerner, AllScripts, eClinical, Athena Health, and NextGen, e-prescriber SureScripts, pharmacy Walgreens, large healthcare organizations Intermountain Healthcare, Mayo Clinic, Baylor College of Medicine, Vanderbilt University Medical Center, and Trinity Health, State HIE's Hawaii Health Information Exchange, Michigan Health Information Exchange, and Wisconsin State Wide Health Information Exchange, associations American Academy of Dermatology, American Academy of Family Physicians, and two Federal Agencies the Indiana Health Services and the Veterans Health Administration. Further, DirectTrust recently created a sub-workgroup to discuss how Direct Secure Messaging can be used to speed the time it takes to get medical records for Social Security Disability claims.

Direct Secure Messaging is a valuable interoperability solution that is currently experiencing exponential growth because Direct Messaging provides value to healthcare organizations and patients.

Removing Direct Secure Messaging from the 2015 Edition would be a major setback in achieving interoperability. We urge the ONC keep the Direct Secure Messaging in the 2015 Edition.

Patient Exchanging Secure Messages with Care Providers

DirectTrust Direct Messaging is a cost effective tool for providing bi-direction exchange of information between patients, providers and payers. Further, non-profit DirectTrust is the ANSI Accredited Standards Development Organization for Direct Secure Messaging.

ADT Messages

Direct Secure Messaging is a standard for the secure bidirectional exchange of medical records nationwide. Direct Messaging can be used to transport any contents including CCD's, HL7 V2 messages, XDM/XDR, and images. Direct Secure Messaging has been implemented as a RESTful API using trigger events to automate processed including referrals, transitions of care, and HL7 V2 ADT (admission, discharge, transfer) message. This eliminates the need for healthcare providers to maintain connect via secure FTP (file transfer protocol) to transmit HL7 V2 ADT messages significantly reducing cost.

Direct Secure Messaging is a valuable interoperability solution that is currently experiencing exponential growth because Direct Messaging provides value to healthcare organizations and patients.

Removing Direct Secure Messaging from the 2015 Edition would be a major setback in achieving interoperability. We urge the ONC keep the Direct Secure Messaging in the 2015 Edition.

View Download and Transmit to a 3rd Party

We do not support the removal View, Download and Transmit to a 3rd Party. Removing Direct Secure Messaging and View Download and Transmit to a 3rd Party from the 2015 Edition would be a major setback in achieving interoperability. We urge the ONC keep the Direct Secure Messaging and View Download and Transmit to a 3rd Party in the 2015 Edition.

Integrating Revised and New Certification Criteria into the 2015 Edition Privacy and Security Certification Framework

We agree with the addition of privacy and security into the 2015 Edition. Further, we recommend that all HealthIT apps be required to implement privacy and security regardless of whether or not HIPAA applied to the HealthIT app (e.g. they are only a patient facing application).

New or Revised Certification Criteria in This Proposed Rule

We agree with the adoption of FHIR; however recommend the adoption of FHIR Release 3 instead of version 2 (the current release of FHIR is version 4.0.0); however, we do not support the removal of Direct Secure Messaging. Further, it might be helpful to create standards that evolve such as the most recently approved version of FHIR in which the ONC would update the version of FHIR that is required with a 12 month notification of the version to allow HealthIT vendors to program to the next version.

FHIR vs. SMART of FHIR

SMART "Substitutable Medical Applications, Reusable Technologies" was created in 2010 by a $15 million grant from the ONC. SMART is managed by Boston Children's Hospital Computational Health Informatics Program and the Harvard Medical School Department of Biomedical Informatics. SMART initially started out defining content of a medical record. SMART is not an ANSI Standards Development Organization.

FHIR "Fast Healthcare Interoperable Resource" was also under development by HL7 "Health Language Seven International". FHIR is an international standard that defines the structure and content of the medical data. FHIR continued to gain world-wide support as the next generation of content standards in healthcare. FHIR is a ANSI Standards Development Organization.

In 2013, SMART decided to pivot to focus on the creating an application layer on top of FHIR known as SMART on FHIR. SMART on FHIR is designed to allow EHR's and health system to choose how applications will interact with data contained in EHR systems. SMART on FHIR allows health systems to choose:

1. Who the EHR and/or health system is willing to share data or which applications will be authorized to have access
2. What data elements will be shared with the application
3. How the data will be shared with the application. To date, all SMART applications have been implemented to be "read only access" and do not allow for bi-directional sharing of data. Further to date most applications using SMART are limited to research-based applications.

SMART is an additional application layer in front of the EHR that is designed to allow health systems the ability control of who, what, and how applications can access the data contained within their EHR system.

SMART uses OAuth2 which works like this: the system that controls the API and data is called the resource server and the server checking authorization is called the authorization server (note they don't have to be separate systems just separate functions). How these two servers interact is not defined in the specification so it is up to each EHR to define. Authorization can be provided by a token or via identification of the user and permission via a cryptographic key.

We are concerned that SMART on FHIR could provide another way for EHR's and health systems to continue data blocking. Further, we are concerned that SMART on FHIR could be biased because it is governed by a healthcare provider organization and not a diverse group of stakeholders. We believe that governance should be via a conscious group similar to HL7 and DirectTrust.

HIPAA Compliant Democratization of Data

What is needed is HIPAA compliant democratization of data by allowing access to patients and HIPAA Compliant entities via standard process that is specified. This means:

1) Every FHIR client application can communicate with every FHIR server application using a standard specification
2) Access to data is based on the credentials of the requestor. These credentials should be bound to the identity of the entity making the request such as patient, healthcare provider, insurer, or device which is bound to a token or cryptography keys that provide non-repudiation of identity.
3) Right to access authorization authority:
    a. Patient or their delegated entity accessing data on behalf of the patient
    b. HIPAA compliant covered entity / treating provider
    c. HIPAA compliant health insurer
    d. HIPAA compliant business associate of a covered entity who meets the definition of operations

This removes the ability of an EHR vendor or provider organization from blocking access to data from individuals or entities to that have the right by virtue of being a patient or granted under HIPAA to access the data.

Further, we believe the DirectTrust Trust Framework for identity proofing and assignment of cryptographic keys can be leveraged to create the trust framework for FHIR by digitally signing the Jason Web Token (JWT) in real time thus establishing trust between to previously unknown entities.

Exchanging Patient Identification Management Within a Community

We disagree with the use of multiple patient identifiers and patching matching. Instead, we propose a single on-ramp be achieved by requiring every entity including patients, the patients' authorized entities, providers, payers and their business associates that have access to or handle PHI and EPHI in health information exchange be Identity Proofed and assigned a trust credential that is bound to a digital identity. This "on-ramp" should also apply to app developers.

- We believe the level of Identity Proofing should be in accordance with NIST 800-63-3 Revision 3 at Identity Assurance Level 2 (IAL2).
    - We recommend that trust credential be bound to a digital identity bound to two key pairs (each key pair has one public and one private key) that complies with Public Key Infrastructure Certificate Internet X.509. Further, that each identity have two pairs of cryptographic keys, one pair is used for digital signature and the second key pair is used for encryption and decryption of data in accordance with FIPS 186.
    - We recommend that the level of encryption comply with FIPS 140-2 Level 2.
    - Further, the cryptographic keys should be stored a Hardware Security Module providing both hardware and software encryption compliant with FIPS 140-2 Level 2.
    - We recommend that instead of using matching algorithms that patients are matched using the cryptographic keys.

Publish and Subscribe

Further, we propose that the digital identity contain the right to access authority such as:

- Patient Accessing Their Own Records
- Treating Provider
- Payer Responsible for Payment
- Business Associate of a Covered Entity

The requestor should be able subscribe to the push notification and be trusted to get the data based upon their trust credential that is bound to their identity and their access authority. The trust credential would provide:

- Nonrepudiation of identity of the patient, provider, payer, or business associate
- Cryptographic certificate that is bound to that identity
- Right to access authority

Listing of Providers for Access by Potential Exchange Partners

An additional electronic endpoint contained in the Directory should be the patients, providers, and payers DirectTrust Direct Address. Note the difference between Direct Protocol and DirectTrust Protocol is that a DirectTrust Direct Address has been identify proofed to NIST 800-63-3 Level of Assurance 3 or higher and this identity has been bound to two pairs of cryptographic keys. One pair is used for digital signature. The second key pair is used for encryption and decryption.

* * * * * *

Thank you for this opportunity to share our input on the ISA.

Sincerely,

Linda Van Horn, BS, MBA
President / CEO
iShare Medical