



ONC

Response to Request for Comments

Connecting Health and Care for the Nation

A Shared Nationwide Interoperability Roadmap

April 3, 2015

Dear Madam or Sir;

We appreciate the ONC's leadership role and work on interoperability. We believe that this work is important for the future of health care ability to reduce the cost of healthcare and improve care and outcomes.

Interoperability has two parts: Transport (including security and trust) and Content (including vocabulary, code sets and syntax).

Transport, Security and Trust

Interoperability is a team sport. To achieve interoperability, there must be a trust framework and transport rules that ensure the HIPAA compliant exchange of data. Critical to this framework is the ability to trust the healthcare organization, EHR vendors, and HISPs. Currently some healthcare organizations, EHR vendors and HISPs choose whether or not to exchange data with other healthcare organizations, vendors and HISPs based on business decisions rather than technical or operational concerns. This is not in the best interest of the greater good.

In addition, some in healthcare organizations, EHR vendors, and HISPs exclude bidirectional exchange of data stating that they cannot trust the end points. This is especially true of exchange of data from patients. In order to reach the full potential of patient engagement, we need ID proof all endpoints including patients. This protects both the patient and the provider.

Historically, trust has been established by DURSA or by trust networks such as DirectTrust. DirectTrust is an organization who through EHNAC accredits HISPs to help ensure compliance with HIPAA Security, Privacy and Breach notification rules and HISP operating guidelines. Once Trust has been established, then the end points can trust the other end points.

It is the policy of DirectTrust to require a high level of assurance or NIST Level 3 ID Proofing. We agree that all end points should be ID Proofed to NIST Level 3. Once ID Proofed, the end point

is assigned a secure credential that can be used identify the end of for trusted exchange of data. Further, an end point needs to be authenticated each session (log in) following NIST Level 3 requirements.

ID Proofing and authentication includes providers, employees or agents of providers, business associates of providers, and patients. End points should be discoverable. We recommend including the end point identification such as the Direct Address for providers to be included in the NPPES data base which can be downloaded and used for data exchange. Allowance should be made for a provider to have multiple Direct Addresses as Direct Addresses are normally assigned based on the provider organization (for example the data primary key is NPI of provider, NPI of provider organization, and Direct Address).

This will allow for bi-directional exchange of data between trusted end points. Further, once ID Proofed, authenticated and following HISP rules for privacy, security and data exchange, a trusted end point should be able to find (query), view, download, update, and transmit health information to another trusted end point over a secure trusted network such as that which has been established by DirectTrust. The source of the data should be clearly identified (data provenance).

At present, the DirectTrust framework is proven technology that works. And, at present FHIR and RESTful API's holds great promise for the future; however there is no normative standard for FHIR. Until such time as a normative standard exists it would not be prudent to require compliance to something that does not exist. In addition, there is no trust framework or governance defined for a RESTful API approach. We encourage the development of a RESTFUL API's and a trust framework for REST as we agree that this approach is the correct technology going forward.

Content, Vocabulary, Code sets and Syntax

The healthcare industry has been interoperable with insurance companies for decades. This interoperability has been made possible by agreement on a common code sets such as ICD-9 (soon to be ICD-10), CPT, HCPCS Level II, CARC (Claims Adjustment Reason Codes), and RARC (Remittance Advice Remark Codes), common format ASC 5010x12 standards, and CORE Operating rules. This is what is needed in health information exchange.

We agree with the ONC's work and encourage clear standards for vocabulary, code sets, and syntax. We agree with the statement on page 10, item 1 that "Electronic health information is not sufficiently structured or standardized and as a result is not fully computable when it is access or received."

We agree upon the establishment of a common clinical data set on page 12, but encourage a common code sets and format be defined including data type (number, alpha, alphanumeric) and character length much in the way 5010 x12 defines their data sets. The code sets used in health information today include, but are not limited to:

3150 Mercier, Suite 608A, Kansas City, Missouri 64111

- CPT
- ICD-9 or ICD-10
- NDC
- HCPCS Level II
- SNOMED
- LOINC
- NCPDP
- RxNorm
- DICOM

We also agree with the inclusion of Prescription Drug Monitoring Programs and suggest that the ONC consider including reviewing work that has already been done by U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration (SAMHSA) as authorized under NASPER (National All Schedules Prescription Electronic Reporting Act) for collecting data from States on prescription drug monitoring for inclusion as a look up item in the clinical data set. Perhaps a bidirectional interface could be created for querying prescription data and updating it when new prescriptions are created.

* * * * *

Thank you for the opportunity to comment on Connecting Health and Care for the Nation
A Shared Nationwide Interoperability Roadmap.

Sincerely,



Linda Van Horn, MBA
President / CEO
iShare Medical