DirectTrust The most trusted name in health information exchange

Comment to ONC on Draft 2017 Interoperability Standards Advisory

As President and CEO of DifrectTrust.org, Inc. (DirectTrust), a large, inclusive, and diverse health IT industry alliance non-profit, I would like to comment on Section III-A of the draft 2017 Interoperability Standards Advisory, Interoperability Need: An Unsolicited "Push" of Clinical Health Information to a Known Destination Between Individuals and Systems.

First, let me comment on the state of adoption of Direct and its significant development as a standard for secure and interoperable health information exchange. The advanced stage of adoption reported on here is in large part a result of the early support that DirectTrust received as the recipient of a Cooperative Agreement with, and funding from, ONC under the "Exemplar Health Information Exchange Governance Entities Program" between 2013-2015. The primary mandate charged to DirectTrust by ONC under the agreement was the establishment of a large "trust community" that would build national scale for the trust relationships needed for provider and patient confidence in sharing of protected health information (PHI), such that individual parties to the exchanges would not need to engage in expensive and time-consuming one-to-one negotiations or agreements regarding policy and controls for privacy, security, and trust in identity, but, instead, would rely upon assurance resting on a common framework of technical standards, trust policies, and best practice requirements, voluntarily agreed to and enforced through: robust accreditation and audit of service providers; a brief legal agreement known as the Federated Services Agreement; and oversight by DirectTrust, its Committees and Board of Directors. I feel it is important to note the success of this governmental-private sector partnership as the foundation of current progress.

The Applicability Statement for Secure Health Transport was initiated as a collaboration between industry and government experts to establish a formal specification for the Direct Project, whose primary goal was to create a simple, secure, standards-based means of interoperably sending protected health information (PHI) over the Internet and between users of different EHR vendors' products. Version 1.0 of what became known as the Direct standard, or sometimes simply Direct, was established through work involving software developers and leading security, identity, and Internet transport experts, with a significant portion of the specification coming directly as a result of code written in an early reference implementation.

Five years into production level use, Direct is a now a proven set of technical protocols for secure interoperable health information exchange based upon secure message transport and an industry-wide Public Key Infrastructure (PKI) and a policy infrastructure maintained by DirectTrust.

Over the years, Direct, the Direct Project, and DirectTrust have evolved to keep up with changes in the industry and technology, and to address questions and issues that have arisen along the way. In the summer of 2012, version 1.1 of the Applicability Statement was published with clarifications around certificate discovery and other small details. Most recently, in late 2015, version 1.2 was published to

1101 Pennsylvania Avenue NW
3rd Floor
Washington, DC 20004

DirectTrust.org
913.205.7968
www.directtrust.org

further clarify ambiguities around Message Delivery Notification (MDN) messaging, intermediate certificate discovery, and usage of cryptographic standards (most notably the requirement of using SHA-2 functions by the message sender) to enhance security and trust. It is import to note that the Direct Project has taken exhaustive care to evolve in a backward compatible manner to ensure interoperability between users of all versions of the protocol all the way back to version 1.0. The Applicability Statement, Edge Protocol, and Reference Implementation have all been updated in 2015, and additional security support was provided in 2016.

Simultaneously, DirectTrust has grown into a robust and continuously improving governance entity supporting both the Direct service provider and end-user communities, providing technical expertise, policy guidance, network infrastructure, and oversight to a large and still growing network of networks for the deployment of Direct messaging and diverse attachments nationally.

DirectTrust's governance and policy framework now rests on the following components and programs:

- Third generation HISP Policy and Certificate Policy documents;
- An updated Federated Services Agreement legally binding HISPs and CAs to terms and conditions inclusive of federal agency participation;
- A highly evolved privacy, security, and identity management Accreditation Program known as the DirectTrust Accreditation Program;
- A Directory and Network Services infrastructure whose components include two trust anchor bundles (the Accredited Trust Anchor Bundle and the Governmental Trust Anchor Bundle), and a Directory Aggregation Service that now includes Direct Addresses and other information on approximately 500,000 identify-proofed individuals and their organizations.

As of the second quarter of 2016, there are 40 DirectTrust accredited HISPs and 15 RA/CAs who together provide Direct messaging services to approximately 300 ONC-certified EHR technology companies and their customers. One of these HISPs is operated by the Veterans Health Administration, and another by the Indian Health Service. Some HISPs are operated as stand-alone service organizations, others as divisions of EHR and PHR vendors, others by HIEs, and still others by health care provider organizations. HISPs also provide Direct services to over 30 HIEs and their members, and to approximately 25 mHealth, PHR, and social website application providers and their customers.

DirectTrust member Health Information Service Providers (HISPs) have contracted as Business Associates to provide Direct exchange services with almost 60,000 health care organizational subscribers, mostly hospitals, clinics, and medical practices, and also with an increasing number of long term post acute care, home health, and other ancillary non-EHR using entities. HISPs have become dynamic facilitators of interoperability for a wide range of customers, able to interface with virtually any edge system, and affordably connecting with many legacy health IT applications to provide real time interoperability for the first time.

Nearly 1.3 million end-points Direct Addresses have been provisioned to personnel at these subscribers' organizations, all of whom have been identity proofed at a strong level of assurance, NIST LoA 3 or higher. Thus, the DirectTrust network of networks is present in all 50 states and includes subscribers using all of the top 50 EHR technology products, and a majority of the other certified EHR products. Included in the DirectTrust Network are hospitals, clinics, medical practices, ACOs, Lab Informations Systems, PAC systems, ECM solutions, Insurance Companies, Disease Registries, as well as new and legacy health IT applications that generate both structured and or unstructured data. These organizations are leveraging the Direct Protocol as a "one to many" interface approach, creating bi-directional versatile secure channels that offer a more cost effective and sustainable approach to health information exchange than the customary single use one-to-one data interfaces that are common to and the status quo in healthcare today.

Today's advanced HISP services can perform many of the functions commonly associated with HIEs and are complementary with traditional HIE approaches. Advanced HISP functionality can be used to leverage incoming or outgoing Transition of Care (TOC) documents to enhance care coordination across the healthcare community, many of whose providers have no EMR nor a need to have one now or in the future. Advanced HISP services can reconcile discrepancies between receiving and sending end points, reformatting data intended for a specific endpoint on demand. This distributed approach to healthcare coordination and exchange offers many users better ease of use as well as creates fewer repositories of data that can be targets for hacking attacks. An increasing number of long term post acute care, home health, and other ancillary non-EHR using entities are beginning to use the Direct Protocol because it is scalable and sustainable.

The number of Direct exchange transactions continues to grow, and now totals approximately 8 million a month nationwide within the DirectTrust network. We have no means to calculate the number of Direct messages and attachments in other, smaller trust communities around the country using Direct, but estimate these may include another 2.5 to 3 million transactions per month.

DirectTrust HISPs regularly test their interoperation with each other, measured by the success with which a sending HISP receives notification that the receiving HISP has received the package and delivered the sent message and attachment to the edge-client application, e.g. an EHR, through both process and dispatched MDNs. Overall, HISP transactions now interoperate at a 99% reliability rate.

2014 EHR technology certification from ONC introduced the Transport Test Tool and the Certificate Discovery tool for conformance validation of Direct Project implementation to the Applicability Statement and The Implementation Guide for Certificate Discovery. These tools were the first publicly available applications that attempted to execute an exhaustive set of test suites mapping back to the specification, vetted by several members of the DirectTrust community during their development and rollout. During the certification process, the NIST and ONC teams were very responsive to comments and bugs reported by the community, greatly improving the quality of the tool. The 2015 versions of the

tools took an enormous leap forward with the introduction of the Edge Testing Tool (ETT) which included several more tests against the core specification as well as including a large number of tests against the Edge Protocol Implementation Guide and The Implementation Guide for Delivery Notification.

All of these tools have become cornerstones of the DirectTrust accreditation process, and in mid-2016, DirectTrust developed our own testing tool to complement the ONC tools. The DirectTrust tools focus on the HISP operating policies that define a very high level profile for a Direct implementation. Test suites in the DirectTrust tool execute test harnesses that go above and beyond the capabilities of the ONC tools, but are targeted at specific DirectTrust policies.

With this information as preface, I would like to offer the authors and contributors of the draft 2017 ISA a number of specific comments from DirectTrust leaders and technical domain experts that relate to the considerations mentioned in Section III-A "Push" Exchange of the Advisory.

Specific Levels of Adoption It is our opinion that the "adoption level" shown in the chart in Section III-A for "Emerging Standard" version 1.2 of the Applicability Statement should be higher than 3 dots, and should instead be at 4 dots. We think the same is true for the IG for Delivery Notification for Direct, which is now widely adopted and part of the interoperability testing schema for DirectTrust's HISPs.

Use of the Term "Unsolicited" Versus "Call and Response" We would like to comment upon the term "unsolicited" that appears in the title of this section of the draft ISA with respect to Direct exchange and its "push" mode of operation. While in theory the conceptualization of Direct as unsolicited messaging has made sense in the past, particularly as a means of distinguishing it from what is generally known as "query" exchange technologies, in the evolving field of practice Direct exchange has become a two-way mode of communication between established trading partners, used in defined care coordination workflows better considered a "call and response" mode. This applies to other use-cases, including that of communications between an Emergency Room professional and a medical practice, or a provider and patient. It is "asynchronous," in the sense that communication is not as immediate as a telephone call. But it is no longer correct, in our opinion, to characterize the use of the Direct standard as "unsolicited" - as this terminology connotes unexpected, unplanned, or even undesired communications, -- from the perspective of the sending and receiving parties. We find this is no longer an accurate designation for Direct exchange and messaging.

Further, as a secure channel for back and forth communications between care coordinating clinical personnel and their organizations, Direct exchange is increasingly being used for solicitation of additional information, that is, as a means of "querying" counter-parties for patient records and their availability. DirectTrust has no quantitative data on the nature or sophistication of the messages exchanged millions of times a month across its network. However, anecdotal information supports the idea that, as one might expect, the use of the technology of Direct exchange is being adapted to the

demands of the clinical environments in which it is being used, and innovations both technical and methodological are occurring in an incremental fashion.

Information on Innovations at the Level of HISP Services We do have information on specific innovations involving Direct that are being instituted by a number of HISPs and their customers in an effort to improve the utility of the Direct services they offer to their health care provider organization customers. New use cases are now regularly being deployed that utilize Direct exchange for the following types of communication: sending disease registry data to repositories; pushing alerts and reminders to providers based on ADT messages received by an HIE or HIO; referral and registration messages for state tobacco cessation programs; communications between providers and pharmacists in the field; queries to and information data returned to Emergency Department personnel on a patient's arrival to the ED; provider to patient communications, including patient-generated data; and many others.

This is a good juncture at which to comment on the use of FHIR and APIs as standards for cross-organizational and cross-IT system exchange of information via what is commonly contrasted with Direct as a "query" or "pull" model.

We are excited about the development of FHIR and the added functionality that open APIs might afford both providers and patients seeking subsets of PHI for a variety of purposes, and that could lead to improved care, enhanced patient engagement, and a better health caring experience.

However, we want to comment that FHIR is still an immature standard, and it is our observation that the community of technical experts now working on FHIR and API development - of which we count many DirectTrust members as participants -- have shown little interest in the use-case for EHR-to-EHR or organization-to-organization FHIR queries. Most if not all of the current developmental work on FHIR is going into the single-enterprise use-case in which a known party who is already able to authenticate to the enterprise EHR system -- either a provider or a patient -- deploys a FHIR query from an application previously granted authorization to use the enterprise or its EHR's API.

We understand this focus. In our DirectTrust workgroup on FHIR, in which we've assembled a group of technologists with both Direct exchange and FHIR expertise, representatives from the companies who are most involved with FHIR have explained how the immaturity of the standard and their companies' resource constraints require that the use-case for inter-organizational queries using FHIR and APIs has been be placed on hold until there is greater agreement with regards to the many complex aspects of single-enterprise deployments of FHIR through RESTful APIs.

A comment worth offering is that Direct HISPs support the XD* edge protocol. This allows trusted input and output using the Clinical Data Architecture (CDA) data structure between Direct Enabled EHR systems. This capability has already achieved the goals of transporting FHIR queries via Direct between any two edge systems nationwide in a trusted identity proofed- manner. As this is push technology,

authorization issues are the responsibility of the sender and need no further consideration. Additionally, DirectTrust HISPs have demonstrated a proof of concept whereby users of the Direct Protocol execute a “secure push” to initiate a patient query of a FHIR API. The patient Direct Address leverages the existing trust and identity aspects of Direct Certificates to authorize and authenticate the pull of a patient’s own data.

Aside from all other considerations, including the value and utility of secure email and Direct transport being available alongside other types of exchange, we believe that for the foreseeable future no other transport standard offers the scope and scale of exchange for the secure movement of PHI across the boundaries of health care organization and health IT vendor system as does Direct exchange. And, in particular, we want to comment that FHIR and open APIs are at the very least several years away from the maturity, reliability, and low cost now available through the Direct standard over the DirectTrust network.