The Office of the National Coordinator for
Health Information Technology

DIRECT SCALABLE TRUST FORUM

SUMMARY REPORT OF FINDINGS

February 6, 2013

Prepared for: Office of the National Coordinator for Health Information Technology
US Department of Health and Human Services

Prepared by: Deloitte Consulting, LLP

Deloitte.

TABLE OF CONTENTS

This page intentionally left blank.

1. INTRODUCTION

Background

The Office of the National Coordinator for Health Information Technology (ONC) launched a community-driven initiative called the Direct Project in March 2010 to specify a simple, secure, scalable, standards-based way for health care providers to send and receive encrypted health information directly to and from known, trusted recipients over the Internet. The resulting Direct Project specification, formally codified in the Applicability Statement for Secure Health Transport, provides exactly that. The specification is a set of guidelines on the interoperable use of existing Internet standards to achieve security, privacy, data integrity, and verification of sender and receiver consistent with the data transport needs for health information exchange. Put simply, this technical specification can enable secure point-to-point health information exchange across the health care delivery system, regardless of geographic, organizational or vendor-related boundaries.

There are special privacy and security concerns when transporting health information, which is both sensitive and protected by law, due to an insecure network like the Internet. To effectively address these concerns, the Direct Project specification (hereon referred to as Direct) uses public key infrastructure (PKI)[1] to protect information exchanged via the Internet through X.509 digital certificates and public/private keys. This means that Direct users (organizations or individuals) cannot send or receive information to or from other Direct users until they have established trust. The process of establishing trust between users involves three basic steps:

1. Users must determine that they want to send information to and/or receive information from the other user.
2. Users must have a way to discover each other's public keys (per the Direct Project's Applicability Statement) so that messages and attachments can be decrypted.

[1] PKI is a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

3. Users must store each other’s trust anchors for use in assuring the validity of each other’s public keys prior to use. Trust anchors can be either the public keys associated with users or, more likely in today’s implementations, the root certificates[2] associated with those public keys.

From a technical perspective, this process can occur several different ways and is relatively simple when Direct users are subscribed to messaging services from the same service provider. However, when users do not share the same system there needs to be a mechanism for exchanging trust anchors and agreement on whatever set of policies are required as a precondition for that exchange. These policy and operational considerations are not addressed by Direct’s technical specification and involve a variety of stakeholders (such as certificate authorities, registration authorities, service providers, technology vendors, health care organizations, etc.). To enable seamless point-to-point information sharing, implementers must collaborate on elements beyond the basic technical specification, including establishing consistent policies and practices on which all stakeholders agree.

The “scalable trust” described above and discussed in this paper refer to the preconditions for creating Direct messaging “dial tone” between two HISPs. These preconditions involve the issuance, management, and use of certificates; the mechanisms for exchanging certificates; and the proper implementation and operation of Direct infrastructure by HISPs. They do not encompass whether two providers have reason to share patients’ PHI. As when a provider sends another provider a fax, these determinations are made by providers separate from the actual transmission and before the provider presses “send”. As stated in the State HIE Direct guidance:

> The fundamental trust basis for directed exchange is between the initiating sender and the final receiver (not between HISPs). A common set of policies will let HISPs automatically recognize each others’ certificates and provide confidence that information will be securely routed to the right recipient, but a provider will ultimately still need to decide to send/receive information to/from another party for patient care or for other reasons allowable under the Health Insurance Portability and Accountability Act (HIPAA).

[2] A root certificate is an X.509 certificate issued by a Root Certificate Authority and used to verify the digital signatures associated with all certificates issued by the HIDP. A root certificate is the top-most certificate of the tree structure of certificates, the private key of which is used to "sign" other certificates. A root certificate is a self-signed certificate that identifies the Root Certificate Authority.

The Forum discussion and recommendations focused on the policies and practices for creating "trust communities," which would leverage a provider "trust bundle" to support transitions of care (TOC) and other types of provider to provider exchange. A separate discussion is occurring in the Blue Button community about requirements for a patient "trust bundle" to support the view, download and transmit requirements of Stage 2 meaningful use. Both groups will pilot mechanisms for trust bundle exchange, so that vendor to vendor exchange will be possible for both TOC and VDT.

The Current State of Direct Implementations

In light of these issues—and the fact that Direct implementers do not agree on common policies or mechanisms for exchanging trust anchors—most Direct implementations only allow users to exchange with other users who subscribe to the same Direct Health Information Service Provider (HISP)[3], resulting in "islands of automation" .

HISPs cite the lack of agreement on a mechanism for exchanging trust anchors and on the common set of trust/security policies that are the precondition for that exchange, as well as concerns related to legal liabilities, as the barriers to providers exchanging patient information with each other via different HISPs. To address these challenges, some HISPs have executed individual, peer-to-peer legal agreements and then have exchanged and loaded the respective trust anchors, giving their users a way to exchange Direct messages with each other. However, creating such one-to-one legal and policy agreements between every possible pair of HISPs will be cumbersome and will impede the pace of Direct adoption. ONC and other participants in the Direct community believe this approach is neither effective nor efficient, and therefore not scalable.

In response, some entities have formed trust communities and/or accreditation bodies[4] united around a common set of operating policies in support of Direct. Trust communities are made up of a variety of health information exchange entities (HIE entities), health information technology vendors, and/or other stakeholders that have established a set of technical, legal, and business standards. These participants

[3] A Health Information Service Provider or HISP is a third-party organization that provides security and transport functions for directed exchange on behalf of senders and/or receivers.

[4] Accreditation refers to a scenario-specific evaluation that assures conformance to a set of common operational standards (that may rely on certified products) and tends to be service focused. An example is identity management using PKI.

agree to uphold and demonstrate compliance through mechanisms established by the community. Such entities can play an important role in establishing trust across HISPs and unaffiliated networks. However, ONC recognizes that these efforts risk fracturing the Direct ecosystem into multiple (albeit larger) trust domains, rather than a unified, interoperable network.

Effective and efficient (i.e., scalable) trust for Direct is needed to enable Stage 2 of meaningful use. ONC's short-term goal is to help the community of HISP vendors reach agreement on and implement approaches for trust anchor exchange and the common policies and practices that are the precondition for that exchange. Given the inclusion of Direct in the 2014 Edition of Certified EHR Technology, ONC anticipates the vast majority of EHR vendors will provide support for Direct exchange within their applications. Moreover, Stage 2 meaningful use includes information exchange requirements for transitions of care and patient engagement. As a result, healthcare providers will expect and need an ability to send patient health information to other providers (and to patients) via Direct regardless of their underlying HISPs.

To that end, ONC contracted with Deloitte Consulting, LLP to host a forum bringing together industry and federal stakeholders. Participants represented a variety of different organizations, including Health Information Service Providers (HISPs), Certificate Authorities (CAs), Registration Authorities (RAs), Electronic Health Record (EHR) vendors, federal agencies, State Health Information Exchange (HIE) Program grantees, trust framework providers/communities, federal contractors, and others (see Appendix A). The purpose of the forum was to reach agreement on policies and practices needed to establish scalable trust across HISPs and trust organizations.

With the end goal of agreeing on recommended policies and practices for Direct scalable trust, participants worked toward the following three objectives:

- Identify and encourage adoption of common policies and practices for identity proofing and certificate management that can be adopted across trust communities. These would be the preconditions for a HISP's trust anchor to be included in a trust bundle.
- Make progress on a common technical mechanism for distributing trust anchor bundles.
- Identify other common business practices or requirements that will avoid, minimize the need for, or simplify trust agreements between HISPs.

Based upon the three goals outlined above, participants worked under the following two assumptions:

- Identified policies and practices will be adopted by one or more trust organizations.
- HISPs will participate in and join these organizations, therefore agreeing to their policies and practices.

With agreed to policies and practices adopted by trust organizations (including trust anchor exchange), broad participation in these bodies by HISPs, and elimination or minimization of the need for HISP to HISP contracts, providers should be able to send each other patient health information easily and securely using Direct, irrespective of organizational and vendor boundaries.

This report summarizes key findings from the forum. It also outlines suggested actions that ONC could take to help the Direct community reach its goal of scalable trust in support of Stage 2 meaningful use.

Forum Format

ONC contracted with Deloitte Consulting, LLP to hold the two-day Direct Scalable Trust Forum on November 29-30, 2012 at the Crystal City Marriott in Arlington, VA. The agenda (Appendix B) allowed for discussion around the following topics:

- Putting “scalable trust” in context – an exploration of what is meant by scalable trust
- Direct-focused trust frameworks/efforts – a review of emerging trust organizations
- HISP privacy and security safeguards/operating policies
- Identity verification and certificate issuance
- Trust anchor distribution mechanisms
- Trust framework business requirements for HISPs

The community agreed to several ground rules. Most importantly, the discussion would focus on how to support real-world implementation of Direct through scalable trust, and not re-litigate the Direct specification or architectural options. As a baseline to help guide the discussion, the community leveraged and responded to the recommended security/trust guidelines released by ONC’s State Health Information Exchange Program.

In addition to sessions on the topics above, the forum also included open space sessions [5] on topics chosen by participants. Open space session topics, key takeaways, and recommendations are located in Table 1.

[5] Based on Open Space Technology, an approach to convening and facilitating meetings that allows participants to determine topics for sessions/meeting agendas and lead discussions.

2. SUMMARY OF FINDINGS

HISP-to-HISP interoperability is vital, yet remains a challenge.

Throughout the forum, the participants' comments and discussions reinforced the view that exchange between HISPs remains a challenge in the industry as a result of policy/legal—rather than technical—challenges and concerns. To address these challenges, some HISPs have entered into one-off legal agreements with peer organizations. Other HISPs, however, have refused to do so. Likewise, some communities have established federated or common agreements across a limited number of participants to reduce burdens. Still, real-world instances of HISP-to-HISP exchange remains fairly rare, as vendors and HISPs struggle to enable exchange while ensuring trust/security and managing their liability risks.

Trust organizations represent a viable path toward achieving scalable trust.

To frame the discussion of scalable trust, presenters walked through a conceptual model (see Figure 1) of how trust organizations (trust communities, accreditation bodies) could establish a common set of policies, procedures, and mechanisms for exchange both within and between their respective members or participants, addressing a relatively narrow set of issues including certificate policies and mechanisms for exchanging trust anchors. In the example in Figure 1, two trust organizations exist in the ecosystem. The trust organizations establish a common set of policies and practices that HISPs must conform to in order for them to participate in their trust community. Once admitted, a given HISP's trust anchor is added to a centrally located cache of all other participating HISPs' trust anchors. This enables each HISP to validate the authenticity of public keys associated with other participating HISPs. Moreover, as shown in the example, trust organizations—by adopting and enforcing mutually acceptable policies—can also enable information exchange between trust communities by sharing access to each other's respective trust anchor store. The large majority of participants agreed that this approach was needed.

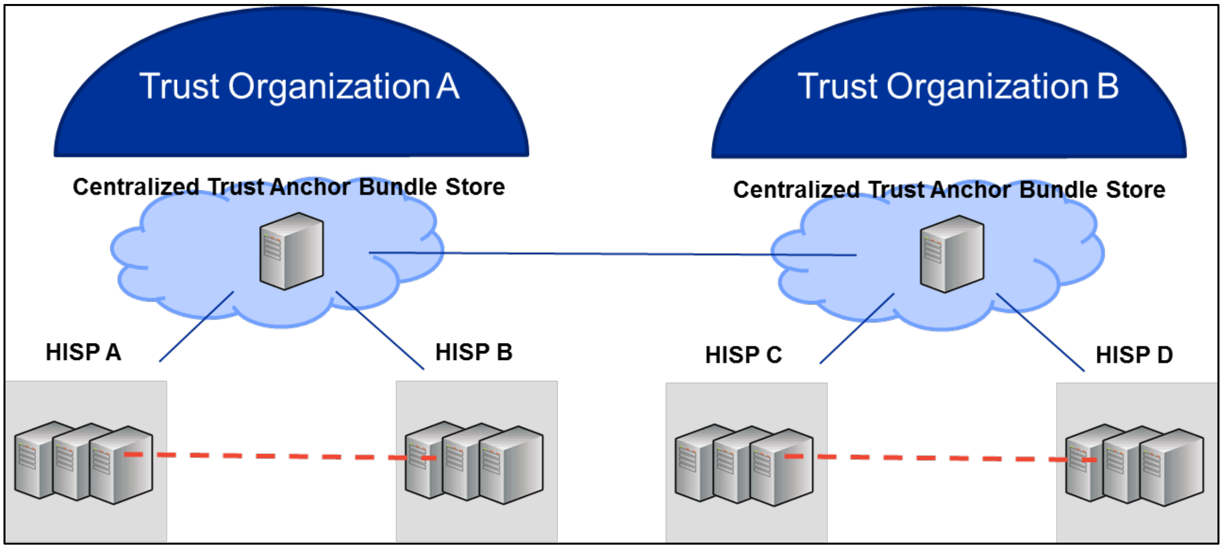
Trust Organization A
Trust Organization B
Centralized Trust Anchor Bundle Store
Centralized Trust Anchor Bundle Store
HISP A
HISP B
HISP C
HISP D

Figure 1. Example of Scalable Trust Model: Peer-to-Peer Reciprocity

Community feedback on the State HIE Program's Direct Security/Trust Guidelines.

As part of the forum's agenda, participants were asked to discuss and provide feedback on the previously published Implementation Guidelines for State HIE Grantees on Direct Infrastructure & Security/Trust Measures for Interoperability. The purpose of these conversations was to understand areas of broad consensus within the Direct community and identify areas in which additional or alternative policy guidance might be desirable. In general, forum participants were highly familiar with and agreed with most elements in these guidelines. Participants asked for clarification or changes in some areas, as outlined below.

Broad consensus around HISP operating guidelines.

Participants were in widespread agreement with recommendations and guidelines around HISP operating procedures and business policies (specifically the State HIE Program's HISP Guidelines 1-5 and 7). On measure #5 (use and re-use of data by HISPs), participants indicated that the restriction was not appropriate where HISPs were simply using information to ensure the accurate transmission of messages but not retaining this information. Participants also asked for transparency through participation agreements and notices of data practices. In addition, participants reached consensus on one recommended enhancement to measure #7 by requiring authentication between HISPs' and providers' systems, in addition to encryption of edge-protocol transmissions between such systems. It was also noted that these guidelines align well with the policies and practices of emerging trust organizations and accrediting bodies (such as DirectTrust.org and the Western States Consortium), although such organizations generally provide more detailed requirements for HISP operating guidelines.

Recommendations for identity verification and certification issuance.

After reviewing HISP operating procedures, the next session was dedicated to the topic of identity verification and certificate issuance. The goal of this discussion was to revisit some of the existing recommendations and guidelines for verifying the identity of organizations and individual providers subscribing to Direct services, beginning with a review of the State HIE Program recommendations for registration authorities (RAs) and certification authorities (CAs).

The vast majority of participants disagreed with the current guidelines for certificate authorities because it restricted HISPs and providers to using certificates directly certified with the Federal Bridge Certification Authority (FBCA). Additionally, participants felt the in-person requirement was unnecessarily burdensome as a baseline to establish sufficient trust for cross-HISP and cross-community exchange.

Forum participants also indicated that there are differences in the way that the FBCA and NIST describe levels of assurance. When the guidance is compared, it does not quite align and can often be unclear. Their lack of alignment presents significant challenges for communicating and aligning across different Direct implementations, trust communities and federal partners.

Based on this discussion, the community had broad consensus around the following recommendations:

- For identity verification, follow NIST Level of Assurance 3 requirements, including both in-person and remote options
- For all other matters related to certificate issuance and management, adopt FBCA Basic (or equivalent) policies and practices.

The group also determined that FBCA certificates should not be required, although some HISPs and providers will use them, especially to support exchange with federal partners.

Implementations based on a single HISP-wide certificate are not acceptable.

The use of single, HISP-wide certificates has been a source of some controversy within the Direct community. To date, ONC and the Direct Project community's position on the matter has been that such deployments do not provide a sufficiently granular level of control for trusting sources/destinations, may lock health care providers into a given HISP (as addresses would not be portable), and ultimately do not conform to the Direct Project community's intent for domain-bound (also known as organizationally-bound) certificates expressed in the Applicability Statement for Secure Health Transport. Participants discussed their views on this matter and reached a clear consensus that single certificates for HISPs are unacceptable.

A common mechanism for trust anchor bundle distribution is needed.

The proposed conceptual model to enable scalable trust and numerous planned/ongoing initiatives are predicated on the exchange of a collection of trust anchors between trusted HISPs (e.g., those that have agreed to policies around authentication, etc.) so that each HISP can locally store the trust bundles for all other trusted HISPs and users can freely send Direct messages to users in those other HISPs. However, a common method for trust anchor bundle distribution is not specified in the Direct Project's Applicability Statement for Secure Health Transport. As a result, trust communities and other entities could establish different means of accomplishing this same task, thereby slowing adoption and creating additional burdens on HIE/HISP/EHR stakeholders and vendors. To avoid this anticipated challenge, participants recommended that the Direct Project community should work together—through a sub-group of the Direct Project's Implementation Geographies Workgroup—to establish a common mechanism and conduct pilots for trust anchor bundle exchange.

A common set of business practices and requirements is vital to avoid or minimize HISP-to-HISP agreements.

On the second day of the forum, the participants engaged in a discussion of the business requirements that HISPs would need to fulfill to avoid or minimize HISP-to-HISP agreements. Participants cited several reasons that HISPs might still need agreements in addition to common policies and technical mechanisms for trust bundle exchange:

- Concern that after one HISP passes a message to another HISP for routing and delivery, a problem occurs and the message is not delivered to the intended recipient (perceived risk/liability).
- Concern that breach safe harbors for Direct are unclear and that the absence of legal precedent creates a certain degree of fear, uncertainty and doubt.
- Need for a mechanism that ensures all HISPs to which a given HISP is routing messages are abiding by the same or equivalent business practices (identity proofing, certificate policies, etc.), including a common enforcement mechanism.
- Need for transparency around additional services offered by HISPs (such as data access, analysis, storage in central repository, etc.) through notices of data practices and end user agreements, as well as clear separation of such services in business operations.
- Need for Business Associate Agreements (BAAs) between HISPs and end users.

Participants agreed that a few steps by HISPs and trust organizations could minimize the need for peer-to-peer agreements.

Recommended Element	Description/Notes
Business Associate Agreement between HISP and end user (most often a health care-related organization)	This must include clearly defined data access / use provisions.
Dispute resolution mechanism among HISPs	Participants discussed the need for this from a conceptual level, but did not delve into the entity or type of entity that would be well suited to oversee or mediate a dispute resolution process.
Explicit transparent accreditation process for HISPs	Would address compliance with a range of policies and standards for HISP business practices and operations (such as information security controls),

Recommended Element	Description/Notes
	but would not test technical services the way certification testing does and would not necessarily replace trust communities/local governance structures.
Auditing/enforcement by accrediting body of HISP's ongoing compliance with established policies and standards	Conducted at regular/standing intervals.
Clarification of breach safe harbor provisions as they apply to Direct and HISPs (as Business Associates of Covered Entities)	This should include an open dialog with the legal community serving HISPs and EHR vendors
Federated trust agreements	*An agreement between an accredited HISP and the trust organization, whereby the accredited HISP attests that it has implemented and will abide by the provisions of accreditation, as well as other terms and conditions associated with participation in the trust community*

Federated trust agreements were added to the list of elements after a discussion of the other elements as a standalone package. Several participants were more comfortable with the complement/package of elements once the federated trust agreements were added, indicating that these provide a more explicit "pledge of allegiance" on the part of HISPs to abide by the accreditation provisions in an ongoing manner. One suggestion indicated that federated trust agreements may be a good starting point for launching the other elements in the package. However ultimately implemented, participants were very clear in their desire to minimize the need for peer-to-peer agreements between individual HISPs.

Concern was also raised that although the conceptual package of elements above sounds acceptable, whether it eliminates or minimizes the need for one-to-one HISP agreements depends in large part on the details of the accreditation program and what is/is not addressed through it. While there was widespread agreement about the need for these steps, there were also many questions about what the specific requirements would be and how they would be implemented. To further specify the details that must be addressed through an accreditation program to minimize the need for peer-to-peer HISP agreements, the

Direct Project community will form an open sub-group of its Implementation Geographies Workgroup in January 2013.

Defining a “glide path” and education are important next steps.

One of the recurring questions that surfaced throughout the forum was, “what do we do in the meantime?” In other words, what are the most important immediate next steps for the community to take as it works towards establishing accreditation, forming trust communities, and developing a mechanism for trust bundle exchange to enable scalable trust for Direct? The most common answer to this question among the participants was education and engagement. This includes not only education for providers, HIT vendors, and state/regional HIE entities on the role they will play in scalable trust to ensure widespread exchange, encouraging rapid formation of trust communities and accreditation bodies and HISPs to join these groups, and also education for and dialogue with the risk management and legal community about security, trust, and liability concerns related to the use of Direct.

Recognizing the importance of this topic, the participants included this subject in the ‘open space’ portion of the forum’s agenda. Details of those discussions are included in Table 1. This session also prompted the formation of an additional sub-group under the Direct Project’s Implementation Geographies Workgroup to outline a “glide path” that will allow the Direct community to take immediate steps that work toward scalable trust while formal accreditation programs and/or trust communities develop. As an important first step, the sub-group will focus on creating transparency by publishing a list of attributes that explain HISPs’ current state of practices and policies (i.e., a registry of HISPs).

Another issue raised was the importance of managing expectations. Participants acknowledged that not everyone implementing Direct will immediately agree to participate in accreditation bodies or trust organizations that will implement the policies and trust bundle exchange practices.

3. CONCLUSION, NEXT STEPS, AND RECOMMENDATIONS

The following sections detail next steps and recommendations based on the outcomes of this forum.

Next Steps and Recommendations for ONC and the Direct Project community

The forum participants identified four action steps for ONC relative to Direct scalable trust:

1. The community asked for ONC to provide guidance to drive HISP policies and Direct accreditation, building from the State HIE guidance and the refinements agreed upon by participants in this meeting. These revised guidelines should be publicly issued in a timely manner.
2. The community asked ONC to develop a lexicon for the Direct community to use in messaging around Direct trust.
3. The community asked for ONC to provide assistance with the education of and outreach to EHR vendors, state HIE entities, providers, legal departments, and other stakeholders on the steps involved in this effort.
4. More broadly, ONC should support the establishment of trust organizations and communities, encourage entities within the market to participate in such organizations, and urge such organizations to establish federated trust agreements to enable widespread, trusted Direct exchange across vendor and organizational boundaries.

The group also proposed the next steps that they, as a community, would take while working alongside ONC, to address the challenges discussed at the Forum:

1. The community will form a workgroup to establish and pilot a common automated mechanism for exchanging trust bundles.
2. The community will form a workgroup to develop a refined “package” of requirements to limit or avoid HISP to HISP agreements.
3. The community will form a workgroup focused on “what to do in the meantime,” specifically focused on immediate steps to encourage and enable interoperability between HISPs.

In concurrence with these workgroups, DirectTrust.org will be completing development of its accreditation process for HISPs in collaboration with EHNAC and other trust organizations.

In addition to the proposed next steps and formation of Direct Project Implementation Geographies sub-workgroups, the group also agreed upon the following timeline:

- February 2013: Complete a set of "Ready to Go" policies, guidance, pilots, and education for vendors/providers.
- April 2013: Accreditation bodies formed, operating, and ready for business.
- September 2013: >50% of HISPs/CAs serving providers for MU2 participating in accreditation.

Recommendations to ONC based on meeting outcomes

As an obligation of hosting this forum, Deloitte Consulting, LLP was asked to draft this report and provide an analysis of the discussion. To that end, Deloitte offers the following observations and recommendations to ONC for its consideration:

1. ONC should address the community's requests for assistance (enumerated above), as well as continue to support the efforts of the community in the Direct Project forum. In particular:

    a. ONC should consider the community's feedback and update its recommendations and guidelines for security/trust in the context of Direct exchange. These revised guidelines should be publicly issued in a timely manner.

    b. ONC should provide additional opportunities for community and vendor education on matters related to health information exchange generally, as well as Direct specifically. This will be increasingly important given the emphasis on data exchange in Stage 2 meaningful use.

2. ONC should support the establishment of trust organizations and communities, encourage entities within the market to participate in such organizations, and urge such organizations to establish reciprocal trust agreements to enable widespread, trusted Direct exchange.

3. ONC should continue to monitor activity within this space and consider reconvening stakeholders, as/if needed, to encourage further progress. In particular:

    a. ONC should monitor for the need for a national governance mechanism. While such regulation has been deferred by ONC in favor of a range of activities to support existing governance activities, some forum participants expressed a desire for a national governance mechanism.

    b. ONC should seek to clarify whether sufficient conditions for trusted Direct exchange may be met through a common accreditation program or whether additional governance (above and beyond established laws and regulations) is needed. This was an area of active dialogue between participants: the interplay between national accreditation programs, e.g. EHNAC, and more localized/regionalized trust communities.

    c. ONC should monitor the alignment of trusted Direct exchange activities both within the provider-to-provider space (the focus of this forum) and in the provider-to-patient realm (which was not explicitly discussed in this forum). Recognizing that different constituencies have different needs, expectations, and requirements.

4. ONC plays a unique role as a neutral convener of interested parties in the Direct Project community. Further, members of the Direct Project community look to ONC for guidance and as a source of legitimacy for their actions in the market. The State HIE Program's Implementation Guidelines for State HIE Grantees on Direct Infrastructure & Security/Trust Measures for Interoperability, as well as the agreements reached in this Forum itself, provide an example of how ONC may quickly and successfully help to encourage industry actions and further dialogue without formal governance. ONC should consider repeating this approach to other domains on interest in the future.

Table 1. Open Space Session Findings

Session Title & Convener	Key Takeaways	Recommendations
"What do we do in the meantime?" – *Lee Jones*	1. We agree with the need to address trust issue with a scalable solution. 2. We do not support HISP to HISP agreements. 3. We understand that we have to be transparent, so we will publish our list of attributes that explain our current state of practice and policies, i.e., a registry of all HISPs that abide by community's guidance.	1. Form an "In the Meantime" workgroup. 2. Draft language/guidance on how to describe this initial step towards interoperability.
Overview of DirectTrust.org – *David Kibbe*	1. DT.org/EHNAC have formed an alliance to develop a national accreditation program for the Trust organizations. 2. Elements of Direct Trust Agent Accreditation Program (DTAAP) will be published by the end of December 2012, and will be taking applications on February 1st 2013. 3. We will have 6-8 accredited entities by March/April timeframe. 4. Rhode Island is going to adopt this accreditation to replace their existing one.	1. Develop education to providers, legal communities, and EHR vendors about accreditation process.
Provider Directories and 360X Project – *Peter Bachman*	1. The trust bar for the developed methodology around referrals and provider directories has been set too high; we would like to lower the trust bar.	1. Find piloting participants for the 360X Project that is supported by ONC.

Session Title & Convener	Key Takeaways	Recommendations
	2. Identity is imperative to know who you're exchanging with and a national framework to structure should be pursued, i.e., HISP or owner of the provider directory should have the authority to verify certificates.	
Mechanisms for distributing trust bundles – *Rim Cothren*	1. There are at least two organizations working through this problem (DirectTrust.org and the Western States Consortium); the group identified overlapping issues and reaffirmed that we're talking about a collection of trust anchors.	1. Must have HISP representation in the Implementation Geographies sub-workgroup on exchanging trust bundles.
EHR-HISP bundling for Stage 2 meaningful use – *Gary Christensen*	1. A good number of the rooms' leaders had not processed the implications of Stage 2 meaningful use for certification participants. 2. There were two items passed forward for the community to think about in terms of how this relates to a business model: I. Encourage the EHR marketplace to adopt XDR. II. There may be creative thinking that will fit within constraints, so we encourage the group and ONC to do this thinking.	1. Repeat the Stage 2 meaningful use webinar that was presented to State HIE grantees for NEHC.
Identity and Agency are NOT health care specific – *Adrian Gropper*	1. If identity or IDP is not applicable across industries, it is the wrong solution. 2. HISPs must be substitutable	1. Group asked ONC to seek clarity moving forward with respect to these two questions.

Session Title & Convener	Key Takeaways	Recommendations
	agents of the licensed providers or data holders.	

4. APPENDICES

Appendix A: Direct Scalable Trust Forum Participants (alphabetically by last name)

Participant Name	Position Title and Organization
Brian Ahier	**President**, *Gorge Health Connect, Inc.*
Peter Alterman	**COO**, *SAFE-BioPharma Association*
Peter Bachman	**CEM**, *PAHISP, LLC*
Lee Barrett	**Executive Director**, *EHNAC*
Nagesh (Dragon) Bashyam	**Chief Architect**, *Drajer, LLC*
Vaibhav Bhandari	**Director of Product Management**, *Optum/United Health Group*
A. John Blair	**CEO**, *MedAllies*
Clayton Bonnell	**Program Specialist**, *US Postal Inspection Service*
Kevin Brady	**Group Leader**, *NIST*
Curtus Browning	**Direct Project Director**, *DoD/VA Interagency Program Office*
Debbie Bucci	**Security Advisor**, *ONC*
Janet Campbell	**Software Developer**, *Epic*
Yvan Charpentier	**Supervisor**, *Interoperability Group, R&D, NextGen Healthcare*
Gary Christensen	**COO/CIO**, *Rhode Island Quality Institute*
Robert Cothren	**PhD**, *Western States Consortium, California Health eQuality*
Farrah Darbouze	**Program Analyst,** *ONC*
Christina DeSimone	**Analyst**, *Deloitte Consulting, LLP*

Participant Name	Position Title and Organization
Barry Dickman	**Senior Consultant**, *AEGIS*
John Feikema	**Coordinator**, *S&I Framework*
John Forrester	**FHA PMO Program**, *IRIS Partners*
Doug Fridsma	**Director**, *Office of Science and Technology*, *ONC*
Erica Galvez	**CoP Director**, *ONC*
Sarah Gornto	**Analyst,** *Deloitte Consulting, LLP*
Miya Gray	**Vice President of Business Management for Directories and Trust**, *Surescripts, LLC*
Adrian Gropper	**Principal,** *Patient Privacy Rights*
Leslie Kelly Hall	**SVP Policy**, *Healthwise*
John Hall	**Direct Project Coordinator**, *Direct Project*
Will Hartung	**CTO**, *Mirth Corporation*
David Hartzband	**Chief Technology Officer**, *Resilient Network Systems*
Andy Heeren	**Director, CERN Network IP**, *Cerner Corporation*
Brian Hoffman	**Lead Associate**, *Booz Allen Hamilton*
Dan Huber	**Product Manager**, *Siemens*
Bob Janacek	**CTO**, *DataMotion, Inc.*
LeRoy Jones	**CEO**, *GSI Health*
Don Jorgenson	**CEO**, DirectTrust CPP WG Co-chair, *Inpriva*
Daniel Kazzaz	**CEO**, *Secure Exchange Solutions*
David Kibbe	**CEO**, *DirectTrust.org, AAFP*
Jeri Kirschner	**Federal Health Liaison**, *Orion Health*
John Lauer	**Enterprise Solution Architect**, *QuadraMed Corporation*

Participant Name	Position Title and Organization
Kat Mahan	**Vice President**, *Araxid*
Vasu Manjrekar	**Director, Enterprise Integration Services***, eClinicalWorks*
Devon Matthew	**Direct Project Manager**, *DoD*
Mark McClellan	**Development Manager**, *ICA*
Gary Moore	**Chief Architect,** *Venafi*
Alice Nyberg	**Project Manager**, *RIQI/DTO*
Ryan Panchadsaram	**Presidential Innovation Fellow**, *ONC*
Christine Phillips	**Technical Manager**, *Florida HIE, Harris Corporation*
Martin Prahl	**Health IT Consultant**, *Social Security Administration*
Joy Pritts	**Chief Privacy Officer**, *ONC*
Kevin Puscas	**Principal**, *NitorGroup*
Matthew Rahn	**Program Analyst**, *ONC*
Scott Rea	**Board Member & Director of Operations**, *Research & Education Bridge Certification Authority*
Will Rice	**Executive Director**, *State of Tennessee*
Carol Robinson	**State HIT Coordinator**, *Oregon Office of Health Information Technology*
Lance Rodela	**Quality Assurance Engineer,** *Medicity*
Jeremy Rowley	**Associate General Counsel,** *DigiCert, Inc.*
Mari Savickis	**Assistant Director of Federal Affairs**, *AMA*
Bruce Schreiber	**CTO**, *MaxMD*
Aaron Seib	**Contractor**, *CalOHII Policy Division*
Avinash Shanbhag	**NwHIN Division Director***, ONC*
Mollie Shields Uehling	**CEO**, *SAFE-BioPharma Association*

Participant Name	Position Title and Organization
Corey Spears	**Director, Standards and Interoperability**, *Aetna*
Walter Sujanksy	**President,** *Sujansky & Associates, LLC*
Bill Sweeney	**Chief Technology Officer**, *IOD Incorporated*
Greg Turner	**CONNECT Product Manager**, *CGI Federal*
Paul Tuten	**Senior Consultant**, *ONC Contractor*
Nick VanDuyne	**Chief Technology Officer**, *New York eHealth Collaborative*
Scott Weinstein	**Presidential Management Fellow,** *ONC*
Claudia Williams	**State HIE Program Director**, *ONC*

The Office of the National Coordinator for
Health Information Technology

Appendix B: Direct Scalable Trust Forum Agenda

November 29-30, 2012

DAY 1

November 29, 2012 9:00 AM – 5:30 PM	
TIME	**EVENT**
9:00 AM – 9:15 AM	**Welcome** Farzad Mostashari, National Coordinator for Health Information Technology
9:15 AM – 9:30 AM	**Putting "Scalable Trust without Governance" in Context** Claudia Williams, State HIE Program Director
9:15 AM – 9:30 AM	**Agenda, Ground Rules, and "What Do We Mean By Scalable Trust?"** Paul Tuten, Senior Consultant, Contractor to State HIE Program
9:30 AM – 10:30 AM	**Overview of Direct-focused Trust Frameworks / Efforts** • DirectTrust – David Kibbe, President & CEO, DirectTrust.org • Western States – Aaron Seib, Founder & President, 2311 • NSTIC Pilot (Gorge Health Connect / San Diego Beacon) – Brian Ahier, President Gorge Health Connect, Inc.
10:30 AM – 10:45 AM	**Break**
10:45 AM – 12:15 PM	**HISP Privacy & Security Safeguards / Operating Policies** Paul Tuten and John Feikema, S&I Framework Coordinator
12:15 PM – 1:30 PM	**Break for Lunch**

November 29, 2012 9:00 AM – 5:30 PM

TIME	**EVENT**
1:30 PM – 3:30 PM	**Identity Verification and Certificate Issuance** John Hall, Direct Project Coordinator and Debbie Bucci, Security Adviser, ONC
3:30 PM – 3:45 PM	**Break**
3:45 PM – 5:15 PM	**Trust Anchor Distribution Mechanisms** Paul Tuten and John Hall
5:15 PM – 5:30 PM	**Closing Remarks for the Day**

DAY 2

November 30, 2012 8:00 AM – 1:00 PM

TIME	**EVENT**
8:00 AM – 9:00 AM	**Day 1 Recap**
9:00 AM – 10:00 AM	**Trust Framework Business Requirements Placed on HISPs** Erica Galvez, State HIE Community of Practice Director, ONC
10:00 AM – 10:15 AM	**Break**
10:15 AM –10:30 AM	**"Open Space" Meeting Set up and Ground Rules Discussion** Erica Galvez, State HIE Community of Practice Director, ONC
10:30 AM – 11:30 AM	**Breakout Session # 1**
11:30 AM – 12:30 PM	**Breakout Session # 2**
12:30 PM – 1:00 PM	**Recap, Next Steps, and Concluding Remarks** Claudia Williams

THANK YOU