DirectTrust Collaborating to Build the Security and Trust Framework for Directed Exchange

Responses to Questions for the HIT Policy Committee's Interoperability and HIE Workgroup Governance Subgroup Hearing, August 22, 2014

from David C. Kibbe, MD MBA, President and CEO of DirectTrust

Please describe the governance approach used to support your information exchange activities. How do you establish and maintain the policy, trust and technical requirements which support information exchange? What issues do your requirements address?

Response: DirectTrust is a non-profit trade alliance that currently has 145 member organizations, and which is self-governing through a Board of Directors, an executive and administrative team, and several committees and workgroups which are led and staffed by volunteers from DirectTrust's membership. Policy, practices, standards used, and technical requirements that support Direct exchange of health information are selected, developed and maintained by a consensual and voluntary approach. Taken together, these constitute a Security and Trust Framework that is the foundation for an accreditation and audit program for Direct service providers, offered in partnership with the Electronic Healthcare Network Accreditation Commission, EHNAC.

DirectTrust accreditation and audit assure that privacy, security, and trust in identity controls in place in Direct service providers and their operations. Accreditation and audit thereby establish an efficient, scalable, national set of trust relationships between and among these Direct services providers, known as HISPs, without the need and expense of additional one-off arrangements and contracts.

So, to be clear, DirectTrust is not in the information exchange business, but, rather in the security and trust business supporting health information exchange via Direct.

Currently, there are 19 fully accredited HISPS and another 28 HISPs in candidate status included in the DirectTrust community and participating in the DirectTrust trust anchor bundles. Together they support over 200 EHRs, provide Direct services to over 28,000 health care organizations nationally, and have provisioned over 420,000 Direct accounts to doctors, nurses, other health care professionals, and health care administrative staff.

DirectTrust is a vibrant, diverse, and collaborative organization that has strong ties to ONC, both because DirectTrust grew out of the Direct Project's "Rules of the Road" Workgroup, and because DirectTrust is engaged in a Cooperative Agreement with ONC under the Exemplar HIE Governance Program. The Cooperative Agreement was first awarded in March of 2013, and then extended for another year in March of 2014. In both years, DirectTrust has been obligated to meet a set of deliverables established by ONC and

available in each year's Work Plan. DirectTrust has to date met these on time and on target. During the first year of the award, there was a grant of $280,000, and during the second year of the award the grant amount was $50,000.

How do you ensure participants adhere to your organizations requirements? What enforcement mechanisms do you have for organizations that are out of compliance with your requirements?

Response: Participation in DirectTrust and in the trust anchor bundles operated for the DirectTrust network is voluntary and governed by an agreement with DirectTrust signed by all participants known as the Federation Agreement. This brief six page document lays out the responsibilities that signatories agree to as members of the DirectTrust community, including very importantly the prohibition against charging transactions fees to each other for the basic transmission of Direct messages and attachments. This agreement also commits DirectTrust to the establishment and management of trust anchor bundles for the common benefit of participants in the community. Breaches of the terms and conditions agreed to in the Federation Agreement by a participant can lead to discontinuation of the agreement by DirectTrust, and removal of the participant's anchor certificate(s) from the DirectTrust anchor bundle(s).

Compliance with the terms and conditions of the EHNAC-DirectTrust accreditation program is the shared responsibility of the accredited entities and both DirectTrust and EHNAC. Non-compliance with accreditation criteria could lead to formal review processes by both DirectTrust and EHNAC, with the possible loss of accreditation status for a party found to be out of compliance. Reinstatement of accreditation status may require additional audit.

Neither DirectTrust nor EHNAC has had occasion to put these enforcement mechanisms into play for members of the DirectTrust community, but they are in place if needed.

How do you manage the evolution of policy and technology requirements (i.e. how do you adopt new standards and retire those that are no longer in use)? What expenses do you experience to govern exchange?

Response: DirectTrust has six active workgroups that meet either weekly or bi-monthly whose responsibilities include the establishment and maintenance of DirectTrust policy and technology requirements on an ongoing basis, including interoperability testing between HISPs and between Direct endpoints such as EHRs and PHRs. DirectTrust also has a Policy Authority one of whose responsibilities is the ongoing monitoring of policy and practices related to security and trust as these are experienced by organizations and people in the field, and for making recommendations to the Board of Directors as conditions warrant. DirectTrust and EHNAC maintain a Joint Steering Committee which meets

regularly to review real world experiences with accreditation and audit, and to clarify or add/remove accreditation criteria as appropriate. Accreditation criteria are published on a yearly cycle, with a sixty day public comment period before final publication.

Both DirectTrust and EHNAC are non-profit corporations acting for the public benefit, and do not seek to make a profit from operations or governance of their policy setting or accreditation activities. Neither organization directly engages in exchange activities.

What, if any, actions should be taken at the national level to help address the governance challenges that are inhibiting the exchange of health information across entities or to mitigate risks to patient safety and/or privacy when exchange is occurring? What role should ONC or other federal agencies play? What role should states play? What role should the private sector play?

Response: In the opinion of DirectTrust leaders, ONC, CMS, and NIST have already taken significant beneficial actions to help address governance challenges that have in the past inhibited the exchange of health information across organizational and health IT boundaries. By supporting both the establishment of health information exchanges at the local, state, and regional level, and by supporting the Direct standard for interoperability and the policy formation and accreditation programs of DirectTrust, these national federal agencies have already significantly mitigated risks to patients' safety and privacy when exchange is occurring.

We would like to see these federal agencies "stay the course" with respect to Direct as a federal standard associated with the Meaningful Use Stage 2 and 3 programs and beyond. While DirectTrust depended upon federal grant assistance to accelerate development of a national, "scalable trust" solution for HISPs and their subscribers through the deliverable of the EHNAC-DirectTrust accreditation program, that financial assistance will no longer be needed after March of 2015 due to the growth in DirectTrust's membership and the contributions from the private sector by members' dues.

However, we believe that the partnership embodied by the Cooperative Agreement between DirectTrust and ONC has significant long term value, primarily in keeping federal and private sector policies aligned, and in persisting a rich dialogue between a now self-sufficient, large private sector coalition dedicated to secure health information exchange, and federal agencies who have a strong and abiding interest in assuring that safety and privacy issues are continually addressed appropriately.

DirectTrust is a vibrant collaborative with a broad range of stakeholders, including HIEs, HISPs, EHR and PHR vendors, state agencies, federal agencies, and health care organizations. Besides its diversity, one of the things that makes DirectTrust noteworthy is that within this membership there are many organizations who compete with one another

in a burgeoning market for Direct services, identity services, security management, and EHR and PHR products. However, they share a common purpose to support the network for Direct exchange, collaborating continuously to improve the reliability, security, and identity assurance for *all* parties who abide by the "rules of the road" that establish trust relationships among them.

Thus, one of the greatest threats to this collaboration would be the ascendence of a dominant vendor, writing its own proprietary rules of the road for interoperability and trust, and forcing these upon a reluctant and captured community whose members would by then have lost the vibrancy of an open and transparent set of processes for establishing these rules through consensus.

We believe it is very important for ONC to pay attention to the market dynamics and allow for multiple solutions to interoperability and trust to flourish, without encouragement of a mono-culture dominated by a single large for-profit corporation, or a small group of for-profit corporations, to impose its rules on the emerging shared culture of health information exchange.

What business practices by providers and vendors are currently blocking information following patients to support patient care?

Response: The business and technical practices in the large majority of HISPs, EHRs, PHRs, HIEs, and their provider organization subscribers nationwide are overwhelmingly supportive of the free and seamless exchange of Direct messages and attachments. They understand that the common benefit of open yet secure exchange is to allow information to follow patients and support care coordination and transitions in patient care. The evidence is very clear that most providers want to be able to make good use of Direct exchange for these use-cases, and are eager to expand Direct to new use cases in the very near future.

However, some EHR vendors have set local policy and practices for the use of Direct by their customers, and in some cases these local policies and practices have the practical effect of inhibiting or blocking entirely the flow of information between providers using Direct. This is even more insidious because in some cases the inbound messages which do not meet the EHR vendor's local policies are "dumped" at the EHR endpoint after passing between the respective HISPs, which can lead to the sending party assuming -- incorrectly -- that the message and its contents were delivered to the endpoint/receiving party. This appears to pose a safety threat to patients, whose care providers may be unable to transfer vital information while also thinking that the content was delivered.

We strongly encourage ONC and CMS to prohibit these information blocking practices to the extent possible, so that all legitimate, trusted Direct messages and attachments are treated equally, and that dispatched MDNs are required so as to notify all sending parties

that either messages are received at the intended endpoint, or have been rejected by the intended endpoint.

Would it be beneficial if ONC monitored the information exchange market to identify successes, challenges, and abuses? If so, what methods of monitoring would be effective; and, what actions should ONC take based upon findings from monitoring?

Response: We would caution ONC to tread lightly in the monitoring of the information exchange market, but encourage all of the federal agencies involved to protect the public interest with respect to privacy, security, and identity, and to assure the free flow of information within appropriate limits. For example, one of the terms of the Federation Agreement that must be signed by all DirectTrust members wishing to have their trust anchors in one of more DirectTrust anchor bundle is the prohibition against charging transactions fees to other relying party HISPs. We jokingly refer to this requirement as the "net neutrality" rule of the road, but it has been very important in establishing that HISPs are not allowed to charge one another for access to their customer base. We would like to see this rule adopted and enforced by other trust communities using Direct and other transport mechanisms. As another example, there is not at present any rule that assures that the sender of a Direct message plus an attachment is notified that the recipient actually received the message. The technical solutions to this dilemma are easy enough to adopt and put into widespread usage, but they are not part of the Applicability Statement at the present time. Finally, the example of "spamming" comes up often, and we would like to be able to assure that HISPs are enabled to stop abuses of this nature by use of appropriate filtering techniques and methods.