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

OFFICE OF THE NATIONAL COORDINATOR

HIT POLICY COMMITTEE AND HIT STANDARDS COMMITTEE

HEALTH INFORMATION EXCHANGE HEARING

JANUARY 29, 2013

PREPARED REMARKS

OF

DAVID C. KIBBE, MD MBA

ON BEHALF OF

DIRECTTRUST.ORG, INC.

The following are prepared remarks submitted by David C. Kibbe, MD MBA, President and CEO of DirectTrust.org, Inc. ("DirectTrust") on behalf of its members and Board of Directors to the Office of the National Coordinator and the HIT Policy and HIT Standards Committees in connection with a hearing on Health Information Exchange held at the Dupont Circle Hotel in Washington, DC on January 29, 2013. We thank ONC and the HIT Policy and HIT Standards Committees for this opportunity to provide testimony and participate in a panel discussion on "Governance Barriers and Opportunities."

Introduction – About DirectTrust

DirectTrust is the successor to the Direct Project "Rules of the Road" Workgroup, incorporated in April, 2012, to serve as a forum and governance body for persons and entities engaged in Directed exchange of electronic health information as part of the Nationwide Health Information Network (NwHIN). DirectTrust is organized as a non-profit, competitively neutral, self-regulatory entity with the goal to develop, promote and, as necessary, help enforce the rules and best practices necessary to maintain security and trust within the Direct community, and to foster widespread public confidence in the Directed exchange of health information.

DirectTrust was established by and on behalf of a voluntary community whose members are interested in health information exchange in accordance with the national standards known as the ONC Applicability Statement for Secure Transport, the ONC XDR and XDM for Direct Messaging Standard, and the ONC Transport and Security Specification, as referenced in the Final Rule for Standards, Implementation Specifications, and Certification Criteria for EHR Technology 2014 Edition at 45 CRF §170.202(a), (b), and (c), effective October 4, 2012.

These standards are together now colloquially referred to as "the Direct standard," deployment of which is often described as enabling "Directed 'push' exchange" or simply "Directed exchange" of health information, essentially secure E-mail with attachments. Directed exchange is, therefore, by definition a form of secure, standards based, inter-vendor sharing of health information over the Internet, between parties who may work in or be associated with unaffiliated healthcare organizations or health information organizations, and who often utilize health IT products and services, such as electronic health records (EHRs), supplied by multiple different vendors.

The primary intention of those interested in Directed exchange is to promote secure, easy to use, ubiquitous, and interoperable point-to-point exchange of health information between providers, and between providers and patients, thereby to improve the quality and safety of care, particularly as part of or related to care coordination, transitions of care management, and patient engagement in health care decisions. DirectTrust and its members view their work as enabling Directed exchange to function smoothly and at scale, thereby promoting improvement in the healthcare system.

At the time of this writing, DirectTrust's active membership numbers forty organizations that include healthcare providers, health IT product and service vendors, certification and identity providers, consumer organizations, state agencies, state Health Information Exchanges (HIEs), and consultants, among others. Membership in DirectTrust is open to a very broad spectrum of healthcare related organizations and individuals, who volunteer their time and effort to support the organization's work and who also contribute through scaled annual membership dues.

DirectTrust originated as the "Rules of the Road" Workgroup chartered under the Direct Project in March of 2011, and is the successor to that Workgroup in both spirit and execution. DirectTrust has carried over from the Direct Project the members' intention of developing a mechanism of industry self-regulation that would be consistent with and would be guided by the principles of the Nationwide Privacy and Security Framework.

By seeking to come to consensual agreement about "rules of the road" for participants and providers in Directed exchange, DirectTrust members have sought to consistently align these rules with existing and developing standards, implementation guidelines, and certification criteria/testing procedures adopted by the U.S. Department of Health and Human Services (DHHS). DirectTrust members have sought to establish rules that are clear, transparent, robust, and obviate the need for complex and cumbersome legal contracting or costly and time-consuming negotiations to occur between and among "trusted agent" service providers such as Health Information Services Providers (HISPs), Certificate Authorities (CAs), and Registration Authorities (RAs), thereby assuring Directed exchange users/subscribers of frictionless and interoperable message exchanges regardless of HISP, EHR technology, or edge client used.

Over time, these "rules of the road" have become policies and best practices requirements, such as the DirectTrust Community X.509 Certificate Policy, which in turn inform a newly established accreditation program, the Direct Trusted Agent Accreditation Program (DTAAP), operated in partnership with the Electronic Healthcare Network Accreditation Commission (EHNAC). DTAAP is designed for trusted agents who wish to voluntarily evidence adherence to them, be recognized for

that adherence, and thereby constitute a single, national trust community for Directed exchange. The benefit of a single national community of trust, all of whose members adhere to the same set of criteria and requirements for privacy, security, and trust in identity, is that of assuring interoperability between and among various implementations of Directed exchange, regardless of geographic, organizational, or technological boundaries.

Although a relatively young organization, DirectTrust has a diverse, rapidly growing membership and its policies and programs are already in active use within the industry. DirectTrust's participating members in many parts of the country are being guided by the policies, interoperability requirements, and business practice requirements that DirectTrust has developed to support and govern health information exchange.

At the time of this hearing, six HISPs, CAs, and RAs who are members of DirectTrust are actively undergoing a beta of DTAAP. Approximately fifteen additional organizations have indicated that they would apply for recognition through DTAAP when it is offered to the public in the first week of February, 2013. We estimate that between forty and sixty HISPs, CAs, and RAs will seek and receive accreditation within this program during 2013.

Governance Opportunities and Successes to Date

The primary message that DirectTrust, its leadership, and its members wish to convey to the participants in this hearing is one of optimism about the ability of the nation's healthcare providers to achieve widespread interoperability of IT systems via Directed exchange by the end of 2013.

While there are still significant barriers to overcome, we are encouraged by the significant progress that has been made to date in realizing the opportunity provided by the Direct standard and its deployment. We are much closer than most people realize to achieving widespread health information exchange over the Internet that is secure, easy to use, and capable of connecting people working in unaffiliated healthcare organizations, health information organizations, and across multiple vendors' products.

The achievement of this goal of universal interoperability has been made much more likely as a result of the requirements for EHR technology certification for Stage 2 Meaningful Use which take effect in 2014. These make it mandatory for EHR technologies to test and certify their compliance with the protocols and specifications of the Direct standard for both sending and receiving of messages and attachments, and their encryption during transport, associated with objectives and measures that relate to both transitions of care and for patient engagement. In other words, the strictly technical capability for customers of these EHR vendors' products to participate in Directed exchange as early as late 2013 is now a foregone conclusion.

One of the reasons that this is so important is that we've learned from experience (with the AAFP Physicians Direct program, for example) that most physicians and other healthcare professionals who use EHRs in their practice would strongly prefer to access Directed message workflow within their EHRs, as opposed to via a website or web portal use of which takes them out of that

workflow. It is a valuable feature of Directed exchange that it may be made available to users/subscribers through a variety of hardware and software endpoints, for example via a website, a smart phone, or a tablet computer, and including providers and patients who don't use EHRs. However, with respect to the attainment of large-scale provider adoption in medical practices and hospitals, the importance of integrating Directed message exchange modules into the EHR interface, much the same way that E-prescribing modules have been so integrated, can hardly be over stated.

The DirectTrust approach takes into account that having the appropriate technology in place for health information exchange to occur between unaffiliated organizations and across multiple vendors' products is critically important. It is a prerequisite for the achievement of national goals for the NwHIN and the Meaningful Use incentive programs. But we also recognize that the technology by itself is not sufficient. Also required are policies on how and when the technology and technique are applied, who the participants are, what roles they play and responsibilities they have, and what evidence has been put forth as to their security practices and trustworthiness. To the extent that those policies are national and scalable – meaning able to be adopted with minimum cost or complexity and to accommodate growth in the NwHIN – then they will complement the best uses of the technology and create the conditions under which we can be confident that an increase in the level of secure electronic exchange of health information will result.

We believe there is room for optimism here, too. The DirectTrust "rules of the road" taken together create a Security and Trust Framework (Framework), operationally defined as a set of technical, business, and legal standards expressed as policies and best practice requirements related to privacy, security, and trust in identity, which the members of DirectTrust have agreed to follow, uphold, and enforce. Key elements of the Framework now in use and which DirectTrust members are increasingly depending upon for Directed exchanges of health information between unaffiliated and/or geographically separate healthcare organizations and across multiple vendors' products, include:

- the DirectTrust Community X.509 Certificate Policy (CP), which describes the unified policy under which a conforming Certificate Authority operates, and specifically, defines the identity vetting requirements and requirements for creation and management of X.509 version 3 public key certificates for use in applications supporting Directed message exchange. The DirectTrust Community X.509 Certificate Policy follows the structure of Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure (PKI) Certificate Policy and Certification Practices Framework (RFC 3647), and is conformant with identity vetting policy from both the National Institute for Standards and Technology (NIST) and the Federal Bridge Certification Authority (FBCA), and;
- the Direct Trusted Agent Accreditation Program (DTAAP), which is operated in partnership with the Electronic Healthcare Network Accreditation Commission (EHNAC), a national healthcare accreditation organization with seventeen years' experience. The DTAAP has been beta tested with six HISPs, CAs, and RAs who currently offer Directed exchange services in two dozen states. The DTAAP was inaugurated to the public as of February 1,

2013, with planned accreditation coverage of service organizations conducting Directed exchange in all fifty states by the middle of 2013.

To summarize, governance efforts for both certification of the technical requirements for Directed exchange as well as accreditation of the privacy, security, and trust in identity requirements for Directed exchange are well underway and capable of being fully established during 2013. Our optimism reflects not only the work that CMS and ONC have done through rules and regulations, but the response of the private sector in showing its willingness to step up to the challenges of creating voluntary, consensual "rules of the road" for scalable trust and as a means of accelerating Directed exchange implementations across the country.

If a public-private partnership, which would necessarily involve other governance entities besides DirectTrust as participants, is allowed to continue to develop and to bring to maturity the policies, interoperability requirements, and business practice criteria that are in their early stages of real world use, we are confident that that national priority of standards based, inter-vendor health information exchange will be achieved within the next two or three years.

Barriers and Challenges Yet Remaining

Directed "push" exchange is E-mail over the Internet between two parties, a sender and receiver, for the purpose of transmitting health information. Each relies on the other for assurance that the identity of the person behind the Direct E-mail address is authentic and valid, and that the privacy of the personal health information contained in the messages and attachments is protected (encrypted) during transport. Each party must have sufficient trust in the other's identity management and security practices to feel comfortable no exposure or breach will take place, accidental or otherwise. Without that trust, exchange cannot be expected to occur on a regular, predictable, and ubiquitous basis, and frequent service interruptions are highly likely.

What constitutes sufficient trust? And how do the relying parties, and the agents acting on their behalf, reach the necessary assurance as to identity, privacy and security, without needing cumbersome one-to-one legal contracts or having to engage in time-consuming and expensive negotiations with one another?

These two questions are at the heart of the mission of DirectTrust and have been the focus of its members' work over the past two years, products from which have already been described and progress noted. However, there remain barriers and challenges that need to be addressed still.

Our experience at DirectTrust in onboarding new members and in speaking to various constituencies about Directed exchange and the conditions for reaching scalable trust, leads us to identify as a barrier the somewhat startling and almost generalized lack of understanding or knowledge about many of the most basic technical and business practice elements of Direct. There is today not widespread knowledge of what Directed exchange can accomplish, nor of what its limitations are. We have found that even highly competent healthcare IT technologists from established companies are often unfamiliar with the domain of identity, credential, and access

management (ICAM) that is central to Directed exchange implementations. Many have some basic understanding of the uses of digital certificates within a Pubic Key Infrastructure (PKI), but are not knowledgeable about the way that the protocols and specifications for Directed exchange operate and implement them. Or, they bring to the discussion incorrect, faulty assumptions about the definitions, roles and responsibilities of the main trusted agents, e.g. Health Information Service Providers (HISPs), Certificate Authorities (CAs), and Registration Authorities (RAs), upon whom Directed exchange depends.

Because widespread adoption and interoperable implementation of Directed exchange by providers and hospitals is linked so tightly to the success of the goals of Stage 2 Meaningful Use, and in particular for transitions of care and for patient engagement, we believe it is a high national priority to find a way to bridge the gap between the current relatively low understanding of what is necessary to mount a secure, interoperable, and trustworthy implementation of Directed exchange, and the much more sophisticated level of understanding that will produce adoption of Direct at scale across the country. This will require an investment in governance related activities to provide technical support, educational outreach, and uses of existing ONC field resources, such as the Regional Extension Centers, to inform service providers, users and subscribers, and the general public about not only how to utilize Directed exchange, but how to assure that its use is secure and protective of the privacy of the messages and payloads that are transported via Directed exchange.

Another barrier that is worthy of mention is that of limiting the liability of trusted agents, HISPs, CAs, and RAs, who provide Directed exchange services to the nation's providers and patients. For most of these service providers HIPAA establishes clear rules for privacy and security. And yet there is a perception that the transport of electronic messages via Directed exchange that will include personally identifiable health information (PIHI) of patients and consumers may place at additional risk the parties who transport the data on behalf of users/subscribers. Movement of data between unaffiliated organizations and across multiple vendors' products – the goal of Directed exchange as a standards based route to interoperability – also raises new questions of liability that have not been encountered due to the newness of the use of technology of Direct.

Questions of liability and particularly indemnification of the parties involved in exchanges of health information have generally been the subject of contractual agreements between those parties. However, as it is a goal of the Direct community and of ONC to avoid the necessity of one-off legal contracts and costly negotiations between HISPs or the individuals and organizations they serve, and to replace those contracts with a mechanism that is more general, shared, and federated with regards to security and trust, there is something of a dilemma here, and a definite tension that needs to be resolved before Directed exchange can become truly ubiquitous and frictionless for its users.

Finally, there is a challenge associated with the development and standardization of user/subscriber directories, often referred to as "provider directories," but, as the optimization of Directed exchange makes clear, such directories may well include end-users who are other than physicians or providers. The goal is to reach a standard approach for use by a national trust community, but there is much work to do to reach that goal.

The Applicability Statement for Secure Transport, the primary technical specification for Directed exchange, lays out a manner for HISPs to expose the digital certificates and public keys of individuals who have been assigned a Direct address, and specifies either DNS or LDAP directory as the means of such exposure to another Direct addressee seeking to send a message. Very minimal information is contained in theses certificates, and in the instance of a Direct organizational certificate, no information about the individual Direct addressee may be the case.

This does not suppose that a member of the public can search for and find a Direct address of a user. Quite the contrary: in order to find the certificate which is bound to a Direct address and available via DNS or LDAP directory, the searching party *must first know* the Direct address of the other party, much the same way that an individual seeking to exchange messages via E-mail in the clear must first know the E-mail address of the intended recipient. There exists no public "white pages" directory for E-mail addresses, nor is there one specified within the Direct standard for Direct addresses.

So, to be perfectly clear, a user/subscriber or "provider" directory is not a prerequisite for Directed exchange to occur in a secure and trusted fashion at scale, and implementations of Directed exchange between parties using separate HISPs and at unaffiliated organizations is now occurring without such a directory in place.

There are, however, use-cases that we can posit that describe how a party wishing to send a Direct message to another party might locate the Direct address of the intended recipient, as well as other information about the intended recipient, and in the absence of such knowledge aforehand. Descriptions of those use-cases may help us to find the best approach to making such information available to willing parties.

For example, there is the use-case in which a user/subscriber of HISP A wishes to "look up" the Direct address of another user/subscriber of the *same* HISP A. There is a demo of a HISP's "provider directory" in action on the Oregon Care Accord (a state sponsored HIE) website located here https://www.careaccord.org/direct-secure-messaging/overview.shtml. We believe, although would need to confirm, that as part of the participation agreement with Care Accord, that the user/subscriber agrees to have some standard set of information made accessible to other user/subscribers of the common HISP. This information might include: Direct address of the user/subscriber, his or her full name, address for associated practice or hospital, medical specialty, preferred format for attachments to Direct messages, and so on.

There is at least one other use-case to briefly consider here, and that is the use-case in which a user/subscriber of HISP A wishes to access and search the user/subscriber directory of a *different* HISP B, and/or vice versa. To some in the Direct community, this is a very important use-case to develop to maturity, because they find it highly desirable that providers, for example those working in an emergency room, are able to "look up" the Direct address of providers working at another institution and users/subscribers of a different HISP.

These and other issues associated with user/subscriber directories, which may serve not only providers but patients and consumers as well, need to be explored in detail. While some people

may be of the opinion that participation in the NwHIN through use of Directed exchange should *obligate* the participant users/subscribers to make public their information of the kind mentioned above, this is a matter of policy and not one that has not been decided in any general or specific way. Lack of clear policy on this particular issue is one among several reasons that provider directories were considered "out of scope" of the Direct Project on more than one occasion.

Summary and Closing

In summary, we would like to thank ONC and the HIT Policy and HIT Standards Committees for inviting DirectTrust to offer testimony and to participate in this panel on health information exchange opportunities and barriers. While it is clear that there is much still to do to effect interoperable health data and information exchange among the nation's providers and with patients and consumers, there is reason to have confidence that by the end of 2013 a significant segment of the healthcare IT industry will have adopted technical standards that will permit their customers to easily and securely send and receive electronic messages and attachments by virtue of their products' integration of the Direct standard, and by virtue of an increasingly clear, transparent, and robust set of policies and best practices describing privacy, security, and trust in identity being put into place by DirectTrust and others. If adopted widely, the latter will obviate the need for complex and costly individual contracts between entities acting as trusted agents.

Remaining barriers to the achievement of this goal include: the still widespread lack of understanding in the provider and vendor communities as to the benefits of Directed exchange and the detailed knowledge necessary to implement the protocols and specifications in a secure and interoperable fashion utilizing a Public Key Infrastructure and X.509 digital certificates; lingering questions among service providers as to the limits of their liability and ways to lessen the risks facing both healthcare professionals and service providers, and; the challenges awaiting the development and standardization of user/subscriber directories which permit willing parties to search and locate Direct addresses and facilitate a broader exchange community using Direct.

With very kind regards,

David Chase Kibbe

David C. Kibbe, MD MBA
President and CEO
DirectTrust.org, Inc.
January 23, 2013