AMERICAN ACADEMY OF FAMILY PHYSICIANS
STRONG MEDICINE FOR AMERICA

June 28, 2012

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Attention: Governance RFI
Hubert H. Humphrey Building
Suite 729D
200 Independence Ave. SW.
Washington, DC 20201

Re: Nationwide Health Information Network: Conditions for Trusted Exchange (Governance RFI)

Dear Dr. Mostashari:

On behalf of the American Academy of Family Physicians (AAFP), which represents more than 105,900 family physicians and medical students nationwide, I write in response to the request for information issued by the Office of the National Coordinator for Health Information Technology (ONC) on the "Nationwide Health Information Network: Conditions for Trusted Exchange" as published in the *Federal Register* on May 15, 2012.

The American Academy of Family Physicians (AAFP) applauds the efforts of ONC to create a voluntary program under which entities that facilitate electronic health information exchange can be accredited, certified, or audited with respect to their conformance to certain transparent and open policies and practices for security and trust. Furthermore, the AAFP appreciates that ONC included in this request for information the ONC established baseline number of "conditions of trusted exchange (CTE)." We share with ONC the belief that a properly crafted governance mechanism inclusive of these elements could yield substantial public benefits. However, we also have significant concerns about specific components of the proposed mechanisms and we offer the following suggestions to improve the nation's Health Information Network further.

In response to the first seven specific questions posed by ONC in this RFI, the AAFP has previously commented in support of the Direct Project, and have shared with the Centers for Medicare & Medicaid Services (CMS) and the ONC our hope that Directed exchange will lead to secure, easy-to-use, and inexpensive health information exchange among providers, and between providers and patients, for the purposes of care coordination, management of transitions of care, and patient engagement. It is our opinion that should Directed exchange become ubiquitous and "worry free" for providers, medical practices, hospitals, patients and consumers, this would represent a major breakthrough for the interoperability of health data exchange.

2021 Massachusetts Ave., N.W. • Washington, DC 20036-1011 • 888.794.7481 • 202.232.9033 • Fax: 202.232.9044 • capitol@aafp.org

In order for Directed exchange to become widely available and "worry free" to our members and their patients, the AAFP believes a number of conditions and foundational activities must take place simultaneously:

1. Direct standard integration with certified Electronic Health Record (EHR) technologies. As the number of providers and hospitals who have adopted and are now using certified EHR technology grows, the tendency is for users to want all of the functionality for care management to occur within the "interface" of their chosen EHR. Therefore, the integration of clinical messaging via the Direct protocols and specifications becomes more and more important with each passing month. The AAFP favors any regulatory activity at CMS and ONC that encourages the market to accelerate the integration of Directed exchange within the EHRs that are certified for use in conjunction with the Meaningful Use incentive programs, and we encourage CMS and ONC to pursue a regulatory course that helps to keep the cost of this integration as low as possible to providers who upgrade or version their certified EHR technology to take advantage of Directed exchange.

2. The establishment and maintenance of a security and trust framework. Directed exchange requires that providers, medical practices, and patients rely on several key "trust agents," among them Health Internet Service Providers (HISP) and Certificate Authorities (CA), in order to maintain security and trust on their behalf. Subscribers of Directed exchange service providers need to have the same confidence in the electronic security and trust policies and best practices in place at HISPs, CAs, Registration Authorities (RA), and any additional vendors employed by these entities, as though they were face-to-face with known and trusted senders or receivers of a Direct message or attachment. In order for this to occur, we believe that industry participants who provide Directed exchange services must be held accountable to a code of conduct that is enforceable, transparent to all parties, and flexible enough to accommodate change, innovation, and competition within the market place. To build this trust, the infrastructure requires not only standards and technology, but also a coherent collective agreement.

3. Predictability in the health information technology market. If there is to be orderly and sustainable growth of Directed exchange in the United States, the market composed of the entities who are essential service providers, e.g. HISPs, CAs, EHRs and Personal Health Records (PHR), must be presented with clear and consistent signals regarding the commitment of the federal agencies involved in promoting health data and information exchange standards. This commitment is also desirable to the potential subscribers and customers, e.g. Health Information Exchanges (HIE) and provider organizations. Lacking those signals, the effects of uncertainty, confusion, and non-standard or arbitrary instances of local governance of Direct, may delay the investments and resources that these venders need to make in order to be ready to meet market demand. Instead, the AAFP advocates for a very high level of predictability that encourages investment by these service providers and accelerates the rate of offering of Directed exchange services. Having a robust infrastructure for Directed exchange in this country may well determine the timeline for Meaningful Use Stages 2 and 3 and any delays in establishment of that infrastructure could unfortunately delay the proliferation of Meaningful Use by several years.

With these three conditions in mind, the AAFP is concerned that the current proposals do not properly "move the ball forward," and we are concerned that the "validation" mechanism as proposed may actually hinder the progress of the adoption and implementation of Directed exchange.

The AAFP is not necessarily opposed to a governance mechanism in which either certification, accreditation, auditing, or a combination of all three, are encouraged and promoted by ONC, and would voluntarily apply to entities that choose to play roles as facilitators of either Direct, Exchange, both, or the innovations and evolved versions of these that will likely occur over time. This kind of recognition program could be of value to the market and the public.

Rather, our concern is that the current proposal contained in this RFI is ambiguous and too broad in its scope to be implemented effectively, and we believe it will likely lead to confusion in the market place just at a time when clarity, consistency, and predictability are needed.

As ONC knows, the AAFP is a founding member of DirectTrust.org, a non-profit trade association which grew out of the Direct Project Rules of the Road Workgroup formed in April 2011. Both the Workgroup and DirectTrust.org have attracted many sincere, enthusiastic, and talented members whose interest is in promoting Directed exchange, that is, in seeing this method of secure Internet exchange between known entities grow in scale, primarily for the purpose of improving management of transitions of care and helping engage patients in their care processes more effectively.

Since November 2011, membership in the DirectTrust.org wiki has grown to over 150 members representing a wide variety of industry entities and organizations who are participants in the Direct community, which includes HIEs, HISPs, EHR vendors, state agencies, CAs, provider organizations, provider membership organizations, consultants, and others. The two main workgroups within DirectTrust.org, the Security and Trust Compliance Workgroup and the Certificate Policies and Practices Workgroup, both have independently and collaboratively worked on many elements of a Security and Trust Framework. One of their goals is to reach broad consensus on a set of policies and best practices which would, when voluntarily adhered to, provide confidence and assurance to Direct participants that mechanisms exist to enforce trust among HISP and CAs in the issuance, exchange, and management of digital certificates that are used in the cryptographic method employed by Direct exchange, which is known as Public Key Infrastructure technology (PKI).

One of the important steps that DirectTrust.org members have taken in this effort is to identify *specific* entities, which may be persons, organizations, or associations, that are participants in Directed exchange as it is actually being implemented in various places around the country, and to reach consensus on the roles, functions, and responsibilities of each of those participants. For example, one such participant is the Subscriber or Direct Addressee, who in some use-cases will be a provider organization or individual, in other use-cases may be a patient or consumer. One of a provider-subscriber's responsibilities is to abide by HIPAA rules and regulations with respect to privacy and security. Another Direct participant is the Certificate Authority, whose function is to issue and manage digital certificates, and among whose responsibilities is to ensure that the processes involved in that issuance and management are in compliance with the Certificate Policy(ies) agreed to by the relying parties, e.g. HISPs and EHRs among others, who utilize the digital certificates in validating the identity of senders and receivers of Direct messages and for the encryption of the messages and attachments.

The AAFP's intent here is not to elaborate upon all of the roles, functions, and responsibilities of the several participants required for a trust community to carry on Directed exchange. However, we do wish to point out that the members of the DirectTrust.org workgroups have been considering very specific entities, their relationships with one another in a chain of trust, and the actual policies and best practices that are required to be followed or adhered to by these entities in order for "trusted exchange" to occur at any scale over the Internet.

It is important to add that much of what constitutes the roles, functions, and responsibilities for participants of Directed exchange have been worked out in PKI architectures in use by other sectors of other businesses outside of health care, for example among the federal agencies and in the aerospace and defense industry. This means that much of DirectTrust.org's work has been to map policies and practices between and across industry sectors in order to not "re-invent the wheel" in applying these to health care, while at the same time attempting to modify and adapt these to the specific conditions and circumstances that health care information exchange demands.

To the AAFP, the concept of a "condition of trusted exchange" only makes sense when it is applied to a very specific, real, and known entity that is a real and actual participant in a trust community utilizing Directed exchange. While the gist of the proposal contained in the RFI suggests a mechanism of governance similar to that envisioned by members of DirectTrust.org, the RFI's proposal would apply to a currently non-existent, poorly defined class of "Nationwide Health Information Network (NwHIN) entities," (NEs) which, if the proposal is finalized as is, must undergo "validation" to become another new class of entities known as NwHIN-validated entities (NVEs). The ambiguity of the definition of what constitutes an NE or an NVE makes it very difficult to determine the roles, functions, and responsibilities these may or may not possess, and therefore makes it more complicated than needed to determine the policies and practices which would apply to each.

NVEs may be a superset, or a subset, of the specific participants needed to carry out Directed exchange, but also may, in fact, be inclusive of entities who do not participate in Directed exchange at all. This new class of entity called an NVE is not a familiar or comfortable construct to us, and feels far too general and vague to be of much help in establishing a workable Security and Trust Framework for Directed exchange, and in some ways threatens to be a distraction from that effort.

We also have concerns with the concept of "validation," and find it confusing and foreign to the actual use-cases within Directed exchange. The RFI makes clear that "validation" may consist of certification or accreditation, including self-attestation, or some combination of these. This does not match well with the AAFP's experience in DirectTrust.org, which suggests that certification, accreditation, and auditing are all processes well known and probably applicable to Directed exchange governance, but which, however, generally apply to different types of products, entities, organizations, and associations.

For example, the AAFP sees a rationale for EHR, PHR, HISPs and other applications involved in Directed exchange, including software modules, to be "certified" as to their capability to perform certain actions that conform to the Direct specifications and protocols. These actions can be tested in much the same way that various parts of the Meaningful Use EHR certification of EHR technologies have been successfully carried out. A Direct-compliant edge client, either a web portal or module integrated into an EHR, can be tested as to whether it can format and send a message using Simple Mail Transport Protocol (SMTP), or employ Cross-enterprise Document Reliable Interchange (XDR). A HISP's software can be tested as to whether it can discover an X.509 digital certificate located in a Domain Name System (DNS) server or Lightweight Directory Access Protocol (LDAP) server. All of the specifications and protocols for Directed exchange can be tested, and successful testing could lead to a "certification" of that capability, much along the same lines that Certification Commission for Health Information Technology (CCHIT) or Drummond now certify EHR technologies for Stage 1 Meaningful Use.

Participants in Directed exchange may also be "accredited" as to their conformance to security and trust policies and best practices within a regional or national trust community. As a matter of fact, several HISPs are already accredited with respect to their security and privacy practices, and there are several other organizations that specifically address health care aspects of security, privacy and confidentiality,

including the sensitive nature of Individually Identifiable Health Information (IIHI) in their accreditation programs. Generally speaking, accreditation programs do not test code, whereas certification programs do test code. And, although there may be significant overlap between the terms accreditation and certification, including the situation in which accreditation requires that a party be or become certified, the two terms have been in common use within many industries for a long time, including within health care and health care information technology.

Finally, the process generally known as "audit" should be considered as one additional method of assuring security and trust with respect to Directed exchange. Audit is differentiated from certification and accreditation in that audits provide only reasonable assurance that statement made or policies claimed to be in operation are free from error, and audits are often performed after accreditation or in the interim between accreditations.

"Validation", on the other hand, is nowhere near as commonly used as certification, accreditation, or audit, and where it is used, as in the software industry, its implications are those of quality assurance and testing for intended use. To our knowledge, the term has never appeared in a single conversation or document within the Direct Project Rules of the Road Workgroup wiki, or within the discussions or documents of the DirectTrust.org wiki, until, of course, the release and publication of this RFI and the proposed process of "validation" become a cause of interest and discussion.

The AAFP's recommendation is that ONC take an approach that:

1. Makes explicit which electronic exchange methodology within the nationwide health information network is under consideration as being the subject of any "condition of trusted exchange," that is, either Direct or Exchange, except in those instances in which a "condition of trusted exchange" may apply to both.

2. Specifies in detail the type and nature of product, individual, organization, or association to which a "condition of trusted exchange" may apply, should apply, or must apply.

3. Recognizes and keeps separate the three classes of recognition and oversight, namely certification, accreditation, and auditing, and makes clear the roles, functions, and responsibilities for which kinds of products, organizations, and other entities which require either certification or accreditation.

We appreciate the opportunity to provide these comments and make ourselves available for any questions you might have or clarifications you might need. Please contact Steven E. Waldren, MD, the AAFP's Director of the Center for Health IT, at 913-906-6000x4100 or swaldren@aafp.org.

Sincerely,

Roland A. Goertz, MD, MBA, FAAFP
Board Chair