



Health IT Policy Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

June 8, 2011

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Mostashari:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

Broad Charge for the Privacy & Security Tiger Team:

The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic HIE, and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to ARRA and the Affordable Care Act (ACA) which mandates a number of duties to the ONC relative to privacy and security.

This letter provides recommendations to the Department of Health and Human Services (HHS) on the issue of the qualification of certificate authorities, which are the organizations that issue digital certificates to health care entities.

Background

An important strategic goal of the Office of the National Coordinator (ONC) is to build public trust and participation in health information technology (IT) and electronic health information exchange by incorporating effective privacy and security into every phase of health IT development, adoption, and use. Stage 2 of Meaningful Use will include requirements to exchange identifiable clinical information among providers for treatment purposes, and these exchange requirements are expected to increase with the advent of Stage 2 and 3. Therefore, the Privacy & Security Tiger Team focused on a trust framework for information exchange between EHR systems, and did not include authentication of individual users of EHR systems. The Tiger Team focused on creating a high level of assurance that an

organization is who it says it is (digital credentials), and that there is an appropriate balance between level of assurance and the cost and burden of implementation.

On November 19, 2010, the Tiger Team made a series of recommendations concerning digital certificates. After making those recommendations, the HIT Standards Committee asked for an elaboration of the recommendation concerning the qualifications of the organizations known as “Certificate Authorities,” which issue the digital certificate. **This letter replaces our previous recommendation #4, in which we suggested that ONC establish an accreditation process for certificate authorities.** Our previous recommendation stated:

Recommendation 4: Characteristics of Who Can Credential/Issue Digital Certificates

- *Any entity willing to assume attendant risks (i.e., be held accountable for achieving a high level of accuracy/assurance) and meet established standards can issue digital certificates*
- *We recommend that ONC establish an accreditation program for reviewing and authorizing certificate issuers*
 - *Annual credentialing of entities is not enough – credential issuers must be required to operate with transparency so their operations can be monitored and problems are quickly identified*

This requirement for accreditation should be evaluated in the context of recommendations from the HIT Policy Committee’s Governance Workgroup.

We are now elaborating on this recommendation and replacing it. In discussing this issue, we first agreed on the following three foundational principles:

1. A high level of assurance with respect to organization identity needs to be obtained.
2. Multiple competitive sources for digital certificates should be available.
3. The certificate should be acceptable to federal agencies, given the frequent need for many providers to exchange information with the federal health architecture.

INITIAL OPTIONS

Because of the highly technical nature of this topic, the Tiger Team formed a separate task force of technology experts, chaired by Dixie Baker and David McCallie. The task force considered three major approaches:

1. The Office of National Coordinator (ONC) establish an accreditation body, as originally recommended, to supervise organizations that issue certificates (“Certificate Authorities”).
2. Certificate Authorities conform to the best practices of WebTrust and/or European Telecommunications Standards Institute (ETSI).
3. Certificate Authorities must be cross-certified with the Federal Bridge Certificate Authority (either directly or chained up to the FBCA).

DISCUSSION OF OPTIONS

The task force came to the conclusion that the third option was the choice that met all three principles. In particular, the task force felt that the second option did not provide a sufficient level of assurance. The task force also felt that, with the third option, a separate accreditation body would not be necessary.

The selection of the third option was based on the following:

1. A high level of assurance is obtained because the identity of each entity applying for a certificate is carefully checked.
2. There are multiple competitive sources for these certificates, and more could be added. We determined that there currently exist approximately six organizations that perform this service and, also, provide reseller capabilities. As a consequence of this competitive environment, the prices for these certificates seem to be reasonable. We determined that these certificates might cost approximately \$50 per year, per healthcare entity.
3. This approach facilitates communication with federal agencies.

The task force also considered whether this approach might represent an implementation burden for small group practices, or other organizations that lack technical skills. Because resellers can obtain these certificates, a practice's EHR vendor can obtain and install the certificate for the practice in the same manner that the vendor performs other technical procedures during installation. Indeed, we learned of one EHR vendor that is already offering that service. Alternatively, for small practices, the certificate can be obtained through an HIE organization or other service provider. Indeed, there are several options for organizations that wish to offer these certificates, which include:

- Certificate Authority cross-certified directly with the FBCA
- Certificate Authority cross-certified with a (new) Health Bridge that is cross-certified with the FBCA
- Certificate Authority cross-certified with an existing Bridge that is cross-certified with the FBCA (e.g., SafeBiopharma)
- Obtain blocks of certificates from a cross-certified Certificate Authority, and resell them to end users under the governance of the Certificate Authority.

We believe that these various structures provide sufficient flexibility so that small practices will have a number of options to obtain certificates, without incurring a significant implementation burden.

S&I FRAMEWORK PROCESS

As noted above, the discussion above was triggered by a request from the HIT Standards Committee to elaborate on the criteria that Certificate Authorities must meet. The HIT Standards Committee also asked the S&I Framework team to investigate the costs and potential implementation burdens of certifying (directly or cross-certifying) to the Federal Bridge. With research provide by ONC, the Tiger Team explored the issue of costs and implementation burdens, and believes that option 3 poses low

cost and could be easily implemented (see the discussion above). However, the S&I Framework is still exploring this issue, and has opened up a brief public comment period.

We agree that it is important to allow the S&I Framework process to continue, so that any lingering doubts or concerns can be resolved through further exploration of the facts. However, we also believe that our recommendation meets the core foundation principles of obtaining high assurance, ability to connect to federal partners, with minimal cost and implementation burden.

RECOMMENDATIONS

We first ask that the HIT Policy Committee endorse the three core principles for ensuring appropriate identity and authentication of provider entities participating in the Nationwide Health Information Network (NwHIN). In our second recommendation, we ask the HIT Policy Committee to replace our previous recommendation #4 with the Federal Bridge option, with a commitment to re-explore this recommendation if new facts on costs and implementation burden are uncovered through the S&I Framework process.

Recommendation 1:

1. Certificates required for exchange under the NwHIN brand should be issued consistent with the following principles:
 - a. A high level of assurance with respect to organization/entity identity needs to be obtained.
 - b. The certificate should be acceptable to federal agencies, given the frequent need for providers to exchange health information with the federal health architecture.
 - c. Multiple competitive sources for digital certificates should be available, in order to ensure that small or less resourced provider entities are able to obtain and use digital certificates.

Recommendation 2:

2. All certificates used in NwHIN exchanges must meet Federal Bridge standards and must be issued by a Certificate Authority (or one of its authorized resellers) that is a member of the Federal PKI framework. The HIT Policy Committee will revisit (or ask the HIT Standards Committee to revisit) this recommendation if the S&I Framework process to further investigate the costs and implementation burdens of requiring cross-certification to the Federal Bridge reveals new facts that call into question the conclusion that it is financially and operationally feasible for small or less resourced provider entities to obtain certificates pursuant to this recommendation.

We appreciate the opportunity to provide these recommendations on the qualification of certificate authorities, and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang

Vice Chair, HIT Policy Committee