Health IT Policy Committee

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

November 29, 2010

David Blumenthal, MD, MPP
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Blumenthal:

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.

Since October 2010, the Tiger Team conducted a number of public meetings and a FACA Blog posting regarding provider authentication. On November 19, 2010, the Tiger Team reported and discussed its findings with the Committee, which were subsequently approved.

This letter provides recommendations to the Department of Health and Human Services (HHS) on the provider authentication issue.

Background and Discussion

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 1 of Meaningful Use includes 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.

The following recommendations apply to provider authentication as part of a measure of network security.

RECOMMENDATIONS

Recommendation 1: Which Provider Entities Should be Issued Digital Certificates?

- All entities involved in health data exchange should be required to have digital certificates
  - Examples of these entities might include:
    - Covered entities
    - Business associates
    - PHR providers
    - Public health entities
    - PBMs
    - Retail pharmacies
    - DME suppliers
    - Laboratories
    - Imaging centers
    - Non-providers--payers, claims clearinghouses, HIOs
    -

[Note: an entity might have multiple entry points]

Recommendation 2: Requirements to be Issued Digital Certificates

- Organizations seeking digital certificates must demonstrate that:
  - They exist as a legitimate business (or a valid business entity)
    - Examples might include: valid licensure, business validity (proof of address/corporate existence), financial account
  - They participate in electronic health care information exchange transactions
- Credentialing organizations/certificate issuers should rely on existing criteria and processes when applicable
  - For example, the NPI
- We did not seek to impose additional privacy and security requirements on provider entities seeking certificates *at this point in time* because we assume privacy and security accountability infrastructure is being developed by the Health IT Policy Committee's Governance Workgroup

Recommendation 3: Process for Issuing Digital Certificates and Process for Re-evaluation

- Multiple credentialing entities will be needed to support issuance of digital certificates given the number of health care entities that will require them
  - For example, vendors and state agencies might be authorized to issue certificates
  - Should also leverage existing processes such as the Federal Bridge

  - Entities such as HIOs that are regionally based and who otherwise have knowledge of the existence of health care providers and entities in their area may be ideal for this function

Digital certificates should contain an expiration date requiring renewal at least yearly or when there is a material change in the evidence originally submitted to justify the issuance of the certificate. Examples of material changes include changes in ownership.

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

Recommendation 5: EHR Certification and Standardization of Digital Certificates

- ONC, through the Standards Committee, should select or specify standards for digital certificates (including data fields) in order to promote interoperability among health care organizations.
- EHR certification should include criteria that tests capabilities to retrieve, validate, use, and revoke digital certificates that comply with standards

We believe that this recommendation to standardize provider certificates and to establish certification criteria represents an important component necessary to achieve greater interoperability between health care entities.

Recommendation 6: Types of Transactions Requiring Certificates

- Authentication is required on any transaction:
  - When the content of the exchange must be protected (due to personally identifiable health information)
  - When the identity of the sender and/or receiver must be known and validated
  - In some cases may only need to authenticate one end versus both
- Examples of transactions that may require authentication of sender and/or receiver include:
  - Transactions that contain personally identifiable health information or may otherwise pose a risk to the patient if the information is not used in an appropriate manner
  - Transactions that would normally be authenticated outside of health care
  - Bulk transactions used to transfer multiple patient records

We appreciate the opportunity to provide these recommendations on provider authentication, and look forward to discussing next steps.

Sincerely yours,

/s/
Paul Tang
Vice Chair, HIT Policy Committee