June 5, 2015

Karen DeSalvo, MD
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. DeSalvo,

In response to policy recommendations from the Health information Technology Policy Committee (HITPC), the Health Information Technology Standards Committee (HITSC) was asked to provide your office with recommendations around the authentication (UA) of *providers* seeking access to protected health information. This transmittal offers these recommendations.

These recommendations are informed by prior recommendations presented by the HITPC, as well as by investigational work performed by the HITSC's Transport and Security Workgroup (TSS WG), which included the identification of gaps in the 2014 Edition Electronic Health Record (EHR) Certification Criteria ("2014 Edition").

Background:

In September 2012, the HITPC provided recommendations on *provider authentication* for exchange of clinical data.[1] The September 2012 recommendations included moving toward requiring multifactor authentication (National Institute of Standards and Technology (NIST) Level of Assurance (LOA) 3) by provider users to remotely access protected health information (PHI); continuing to identity proof providers in compliance with HIPAA; and continuing to be informed by the National Strategy for Trusted Identity in Cyberspace (NSTIC) initiative.

In September, October, and November of 2014, the TSS WG discussed issues related to user authentication and authorization. Several experts presented testimony on topics such as Trustmark technology (from the Georgia Tech Research Institute), OpenID Connect, and identity management work being performed by the NIST that included revisions to Special Publication 800-63 version 2.[2] The TSS WG also received testimony regarding Blue Button Plus, OAuth 2.0, and User Managed Access (UMA), insights from which will be applied to future recommendations.

From these discussions, the TSS WG identified gaps and possible enhancements in the current 2014 Edition Certification Criteria. For example, there is no current requirement in the criteria to protect

[1] See HITPC Transmittal Letter of September 26, 2012, available at: http://www.healthit.gov/sites/default/files/transmittal_092512_pstt_recommendations_provider_authentication.pdf.
[2] See Electronic Authentication Guideline, NIST Special Publication 800-63-2, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.

information that is used to authenticate users (i.e. passwords may be stored in the clear). The TSS WG presented its recommendations to the HITSC on December 10, 2014.

The recommendations presented herein fall within the 2014 Edition requirement to "verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed."[3]

Recommendations:

To strengthen the authentication currently certified in EHR technology, the HITSC recommends adding the following criteria:

- Continuously protect the integrity and confidentiality of information used to authenticate users, using the standard specified in § 1750.210(a)(1) of the 2014 Edition EHR Standards, Implementation Specifications, and Certification Criteria.

Additionally, to enable EHR technology to be certified for having implemented multi-factor authentication, the HITSC recommends adding the following certification criterion:

- For one or more configurable functions, enable a system administrator to configure the technology to require that at least two distinct forms of authentication (which may include knowledge of a secret, possession of a physical object, or possession of a biometric) be presented as verification that a person seeking access to those functions is the individual associated with the unique identifier, as claimed.

The HITSC further recommends that ONC perform the following activities:

- Support the National Institute of Standards and Technology (NIST) effort to revamp NIST Special Publication 800-63-2 (Electronic Authentication Guideline) by:
    - Closely following the move from LOA to componentized trust;
    - Recommending appropriate identity-proofing for query-based access; and
    - Reaching out to NIST for a presentation on security risk management and the role it plays in security policy and technology.
- Track development and piloting of new and emerging technology specifications such as Data Segmentation for Privacy (DS4P), for enabling compliance with legal requirements for segmentation, and the User Managed Access (UMA) profile of OAuth 2.0 for obtaining consumer consent.

[3] See 42 C.F.R. § 170.314(d)(1)(i)

We appreciate the opportunity to provide these recommendations and look forward to discussing next steps.

Sincerely yours,

/s/	/s/
Jon White	John D. Halamka
Chair, Health IT Standards Committee	Vice Chair, Health IT Standards Committee