



# Trusted Identity of Providers in Cyberspace

**A Joint Hearing of the HIT Policy  
Committee, Privacy and Security Tiger  
Team and the HIT Standards Committee,  
Privacy and Security Workgroup**

**July 11, 2012**

# Previous Tiger Team/HITPC Recommendations

1. Organizations that are seeking to exchange information as part of the Nationwide Health Information Network (NwHIN) should be required to adopt baseline user authentication policies that require more than just user name and password for remote access. At least two factors should be required. Remote access is defined as access over a public network like the Internet.

Source: Recommendations were in the context of authentication of individual users (providers) of certified EHR systems. See HITPC Transmittal Letter, dated April 18, 2011; available at: [Privacy & Security Tiger Team Recommendations Transmittal Letter \[PDF - 537 KB\]](#)

## Recommendations (con't)

Rationale for recommendation #1:

- The Tiger Team was not comfortable with requiring the application of the NIST or DEA requirements for EHR user authentication because of the stringency of the second factor requirement.
- The Tiger Team was particularly concerned about remote access (vs. access within an entity's private network), but had a difficult time initially setting parameters for what constitutes "remote" access.

## Recommendations (con't)

2. These recommendations are intended to set a baseline for user authentication; organizations and entities can adopt more stringent requirements.
3. For more sensitive, higher risk transactions, an additional authentication of greater strength subsequent to an initial authentication may be required, as has already been recognized with the DEA policy covering prescribing controlled substances. Additional work may be needed by the Policy Committee and ONC to identify the potential use cases that might require authentication above the baseline requirement.

## Recommendations (con't)

4. NwHIN Policies should be re-assessed for consistency with other national identity efforts, technology developments, such as National Strategy for Trusted Identity in Cyberspace. Such policies should be re-assessed to address innovations in technology both within and outside of the healthcare sector.
  - HITSC Privacy and Security Workgroup has consistently stressed the need for policies and standards at sufficient level of assurance to enable trusted exchanges between private and public sector healthcare organizations

## Recommendations (con't)

5. ONC should also work to develop and disseminate evidence about the effectiveness of various methods for authentication and reassess NwHIN policies accordingly.
6. For writing e-prescriptions for controlled substances, Certified EHRs should have capability for two-factor authentication, at a minimum consistent with DEA rule.
  - HITSC Privacy and Security Workgroup did not recommend EHR standards and certification criteria to support two-factor authentication for Stage 2 meaningful-use (2014), awaiting guidance from DEA