October 2010

On behalf of the Confidentiality Coalition, here are our comments on provider-entity authentication.

In general, HHS/OCR has consistently referred to NIST standards as guidance for complying with HIPAA and HITECH mandated security requirements for securing patient data. NIST guidance is clear, represents industry best practices and government agencies are required to adhere to it. Therefore, it seems reasonable to specify their use for secure authentication with respect to Electronic Health Records.

1. **What strength of provider-entity authentication (level of assurance) might be recommended to ensure trust in health information exchange (regardless of what technology may be used to meet the strength requirement)?**

   The level of assurance is based upon the consequence of an authentication error or the misuse of credentials. Based upon NIST SP 800-60 Vol. 2 guidance, the impact of the loss of confidentiality or integrity of patient medical records is moderate and equates to assurance level 3. NIST SP 800-63 Electronic Authentication Guideline specifies a minimum of two authentication factors (there are three possible authentication factors: something you have, like a token; something you know, like a password; something you are, like a fingerprint) for level 3 assurance. Two factor authentication is rapidly becoming standard in the healthcare industry, is required for government agency use in the State of California when accessing patient records, and would appear to be the most appropriate choice here.

2. **Which provider-entities can receive digital credentials, and what are the requirements to receive those credentials?**

   Access to patient data and therefore, digital credentials granting that access, must be limited to those specifically authorized by the HIPAA regulation (Covered Entities and their Business Associates with current Business Associate Agreements, or a Data Use Agreement in the case of a Limited Data Set) and should only be granted to those with a demonstrated need for such access.

3. **What is the process for issuing digital credentials (e.g., certificates), including evaluating whether initial conditions are met and re-evaluation on a periodic basis?**

   Credentials should be issued pursuant to registration and identity proofing guidance for assurance level 3 in NIST SP 800-63 Electronic Authentication

Guideline. For example, as Jeff Barnett suggested, the Credential Service Provider would be required to –

- Verifying the legal, physical and operational existence of the entity
- Verifying that the identity of the entity matches official records
- Verifying that the entity has properly authorized the issuance of the certificate
- For re-evaluation, a recommended renewal frequency of 12 months.

4. Who has the authority to issue digital credentials?

Assuming the credentials are based on digital certificates, the authority to issue digital credentials must be restricted to Certificate Authorities whose identity proofing and certificate issuance processes are cross-certified with the Federal Bridge CA and mapped to Federal PKI Certificate Policies which are approved for assurance level 3. This requirement and guidance for mapping policies to assurance levels are defined in NIST SP 800-63 Electronic Authentication Guideline. The credentials provide proof of who they are; each Covered Entity/Business Associate still must determine to whom they would extend "trust" for access in the provider-entities' space.

Credentialing using a protocol other than a digital certificate should be allowed, but that they be required to comply with an established guidance, and that they then comply with strict standards, that their credentialing protocols be made publicly available and that they be audited on a regular basis by an independent external auditor (controls similar to those applied to Certifying Authorities for digital certificates).

5. Should ONC select an established technology standard for digital credentials and should EHR certification include criteria that tests capabilities to communicate using that standard for entity-level credentials?

ONC should not direct the use of a specific technology. Each organization should be allowed to select the most appropriate technology for their situation. NIST SP 800-63 Electronic Authentication Guideline requires an organization to complete a risk assessment, map identified risks to the appropriate assurance level, and then select a technology that satisfies the technical requirements of that assurance level. A reason for preempting that guidance and creating a one size fits all approach for EHR access is not apparent.

6. What type of transactions must be authenticated, and is it expected that all transactions will have a common level of assurance?

All transactions involving the disclosure of ePHI must be authenticated to the same level of assurance as indicated in (1), above.