## PSTT02: How would ONC test the HITPC’s recommendation in certification criteria?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Comment ID | PSTT02 | Name of Respondent | Organization | Observation |
| 1 | [HHS-OS-2012-0007-0388](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0388) | p. 1 |   | Crowe Horwath LLP | * Recommended an iterative and phased testing program that spans the population of organizations.
* Recommended an independent verification of adoption for attestation purposes.
 |
| 2 | [HHS-OS-2012-0007-0397](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0397) | p. 12 | Alice Borrelli | Intel Corporation | * Recommended that Electronic Health Record (EHR) certification criteria should include requirements for the EHR to interact with National Strategy for Trusted Identities in Cyberspace (NSTIC) “Identity Providers” during authentication.
* Recommended that credentials used in these authentications be multi-factor.
* Recommended that hardware assisted 2-factor authentication solutions be recognized as suitable multi-factor authentication solutions.
 |
| 3 | [HHS-OS-2012-0007-0425](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0425) | p. 13 | Willa Fields, Stephen Lieber | HIMSS | * Stated the EHR technology has the capability to be configured to require two factors under specified conditions before the user is allowed to perform the requested action.
* Commented that EHR technology has the capability to detect the above-mentioned specified conditions and confirm user identity using at least two factors before allowing the requested action to be performed.
* Commented about the need to determine whether the two factor recognition be native to the application or as a hand-off authentication from the operating system.
* Commented about the need for coordination of vendors to allow such recognition or a standard that would allow "certified" two factor credentials to be passed and accepted.
 |
| 4 | [HHS-OS-2012-0007-0412](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0412) | p. 14 | John Travis | Cerner Corp. | * Commented about a need to define a single standard for use with the credential providers.
* Commented about the need to avoid a plethora of optional NSTIC standards, if more than one standard emerges, ONC should ask the Health Information Technology Standards Committee (HITSC) to select the smallest possible subset necessary for healthcare certification.
* Commented about the Drug Enforcement Agencies’ (DEA) Interim Final Rule as being a good example.
 |
| 5 | [HHS-OS-2012-0007-0376](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0376) | p. 19 | Sarah Cottingham | Telligen Iowa HIT Regional Extension Center | * Recommended using guidance from National Institute of Standards and Technology’s (NIST) 800-63.
 |
| 6 | [HHS-OS-2012-0007-0382](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0382) | p. 34 | Cheryl Peterson/Karen Daley/Marla Weston | American Nurses Association | * Deferred to the Alliance for Nursing Informatics (ANI) response to this question.
 |
| 7 | [HHS-OS-2012-0007-0398](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0398) | p. 4 | Randy Vanderhook | Smart Card Alliance | * Commented about using existing standards such as NIST SP-800-63-1, NIST FIPS-201, Homeland Security Presidential Directive 12 (HSPD-12).
 |
| 8 | [HHS-OS-2012-0007-0391](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0391) | p. 4 | Karen Boykin-Towns | Pzfizer Inc | * Supports recommendations for two-factor authentication.
* Commented about how EHR capabilities should include DEA authentication requirements for prescribers.
 |
| 9 | [HHS-OS-2012-0007-0429](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0429) | p. 6 | Deven McGraw | Center for Democracy and Technology | * Stated that certification should focus on testing the approach that the vendor has implemented and making sure that it functions as intended and minimizes risk.
* Commented that certification requirements should specify that vendors describe the functionality of their solutions fully.
* Suggests considering to provide vendors with certification “credit” if they have implemented a second or third factor that is listed in the most recent version of NIST 800-63.
 |
| 10 | [HHS-OS-2012-0007-0525](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0525) | p.1 | David Finn | Symantec Corp. | * Supports multi-factor authentication under certain, specified conditions.
* Stated that EHR technologies have the capability to detect the specified conditions and then confirm the user identity using at least 2-factors before the requested action is allowed.
* Commented about how the NIST standard for 2-factors should be reexamined in light of new technologies.
 |
| 11 | G:\Meaningful Use\HITPC\Stage\_3\_RFC\Submission | p.1 |   | VA | * Invalid link. Could not view document.
 |
| 12 | [HHS-OS-2012-0007-DRAFT-0051](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0051) | p.1 | Peter Alterman | SAFE-BioPharma Association | * Commented about how ONC could complete a review of the reports sent to the US Federal Public Key Infrastructure (PKI) Policy Authority or the United States Chief Information Officer’s (CIO) Council Federal Identity, Credential, and Access Management (FICAM).
 |
| 13 | [HHS-OS-2012-0007-0210](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0210) | p.11 | Linda  Brady | ADHI | * Commented that written policy should outline the two factor (or higher) authentication process.
 |
| 14 | [HHS-OS-2012-0007-0542](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0542) | p.2 | Jim  Williams | Daon | * Commented that certification criteria can be developed following NSTIC/Identity Ecosystem Accreditation Standards as they are being developed.
* Commented that multi-factor authentication is required.
 |
| 15 | [HHS-OS-2012-0007-0342](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0342) | p.2 | Adolph  Maren Jr. | Oklahoma Health Care Authority | * Commented that EHR vendors using third party credentials would point to certification of the credentialing entity.
* Commented about how EHR vendors using two factor (or higher) authentication would show this in their EHR product test documentation.
 |
| 16 | [HHS-OS-2012-0007-0565](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0565) | p.21 | Leigh  Burchell | Allscripts | * Recommend that this multi-factor authentication not be included in Meaningful Use (MU) Stage 3.
* Stated that when it is included in future stages that it is carefully reconciled with other regulations that require multi-factor authentication.
* Recommended that attestation be used for how the EHR integrates with the two-factor technology.
 |
| 17 | [HHS-OS-2012-0007-0493](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0493) | p.27 | Thomas Merrill | New York City Department of Health and Mental Hygiene | * Requested further clarification as to the type of testing referred to in this question.
 |
| 18 | [HHS-OS-2012-0007-0350](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0350) | p.3 | Landon  Combs | Highlands Physicians Inc | * Suggested asking yes or no questions to verify system set up with appropriate back up documentation provided.
 |
| 19 | [HHS-OS-2012-0007-0499](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0499) | p.3 | Tine Hansen-Turton | National Nursing Centers Consortium | * No comment.
 |
| 20 | [HHS-OS-2012-0007-0315](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0315) | p.32 | Angela  Jeansonne | American Osteopathic Association | * No comment.
 |
| 21 | [HHS-OS-2012-0007-0568](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0568) | p.33 | Sasha  TerMaat | Epic | * Commented that vendors should attest to having an architecture supporting third-party authentication and demonstrate two examples.
 |
| 22 | [HHS-OS-2012-0007-0212](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0212) | p.34 | Kari  Guida | Minnesota Departmnet of Health | * No comment.
 |
| 23 | [HHS-OS-2012-0007-0343](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0343) | p.38 | Donna  Sledziewski | Geisinger Health System | * Commented that functional testing includes demonstration of the use of two-factor authentication and the methods used.
 |
| 24 | [HHS-OS-2012-0007-0332](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0332) | P.4 | Patrick  Sullivan | Harris Corporation | * Suggested that test scenarios should be designed wherein a subject supplies validated credentials and attribute claims to a relying party who validates the credentials and attributes and performs that transactions requested.
* Commented that vendor may act as an identity provider or attribute provider, they may not. In such circumstances, the testing apparatus would accommodate a network call to the third party identity provider and/or attribute provider to validate the presented credentials and attributes.
 |
| 25 | [HHS-OS-2012-0007-0588](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0588) | p.45 | Gregory  Rivas | UC Davis Medical Center | * Commented that this requirement may be creating an additional barrier.
 |
| 26 | [HHS-OS-2012-0007-0333](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0333) | P.50 | Koryn  Rubin | American Association of Neurological Surgeons and Congress of Neurological Surgeons | * No comment.
 |
| 27 | [HHS-OS-2012-0007-0541](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0541) | p.50-51 | John  Glaser | Siemens Healthcare | * Suggested that this domain is not mature enough for certification.
* Commented that as the domain matures this domain should be addressed in a way that is consistent with other regulations, such as the Drug Enforcement Agency (DEA) regulations for e-prescribing of controlled substances.
 |
| 28 | [HHS-OS-2012-0007-0145](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0145) | p.53 | Nancy  Payne | Allina Health | * Suggested checking for enablement of federation language standard – e.g. SAML, in access and authentication functions, or the ability to accept requests from such a system.
 |
| 29 | [HHS-OS-2012-0007-0295](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0295) | p.6 | Susan  Owens | Memorial Healthcare System | * Suggested hat a simple checklist of questions to test for the use of the defined Federated Authentication model could be created and used for certification criteria.
 |
| 30 | [HHS-OS-2012-0007-0327](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0327) | P.6 | Megan  Howell | Group Health Cooperative | * Commented about identifying all areas of remote access, to include internet-facing access or access from untrusted networks.
* Suggested identifying authentication mechanism used when connecting from an untrusted network to the trusted EHR environment.
* Commented about ensuring authentication mechanism is two-factor, using two of the three forms of authentication (Something you have, Something you know, Something you are).
* Commented about verifying that the authentication method as well as the session it established are securely encrypted.
 |
| 31 | [HHS-OS-2012-0007-0520](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0520) | PDF2 - p.78 | Andy Riedel | NextGen Healthcare | * Recommended that this criterion not be included in Stage 3.
* Commented that if it is included in future stages that it is reconciled with other regulations that require multi-factor authentication, such as the DEA Electronic Prescription of Controlled Substances regulations.
* Recommended attestation be used for how the EHR integrates with the two-factor technology.
 |
| 32 | [HHS-OS-2012-0007-0547](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0547) | tab 3 | Erin  Laney | Intermountain Healthcare | * Commented about developing a model audit protocol for the community to utilize as they self-test appropriate certification criteria.
* Stated that control requirements are defined for appropriate audit and credential issuance criteria by 41 CFR Part 11.10. Subpart B (e) and might be considered a basis for developing test objectives in such an audit protocol.
* Stated that there are several digital identity and digital signature and digital security standards that could be used for certification criteria for issuance of a valid third party credential to include standards set by ONC itself.
 |

**Summary**

**Number of Comments:** 26 (6 commenters did not include a response or link was invalid)

**Summary:**

**Test Procedures:** Several commenters made specific suggestions around possible test procedures for the HITPC recommendation in the certification criteria.

* One commenter suggested that the certification criteria be developed following the NSTIC/Identity Ecosystem Accreditation Standards as they are being developed.
* Two commenters suggested use of a checklist or yes/no questions to verify the system set-up, while also requiring for appropriate documentation.
* Two commenters suggested that vendors could be required to attest to having an architecture that supports third-party authentication and be capable of demonstrating two examples.
* One commenter suggested that test scenarios should be designed where a subject supplies validated credentials and attribute claims to a relying party who validates the credentials and attributes and performs that transactions requested.
* One commenter suggested checking for enablement of federation language standard – e.g. SAML, in access and authentication functions, or the ability to accept requests from such a system.
* One commenter suggested the development of a model audit protocol for the community to use to self-test. The commenter notes that stated that control requirements are defined for appropriate audit and credential issuance criteria by 41 CFR Part 11.10. Subpart B (e) and might be considered a basis for developing test objectives in such an audit protocol.

**Functionality:** Two commenters provided recommendations for specific functionality to be tested as part of the certification criteria.

* Two commenters suggested that EHR technology has the capability to be configured to require two-factor authentication under specified conditions before the user is allowed to perform the requested action.
* Two commenters suggested that EHR technology has the capability to detect the above-mentioned specified conditions and confirm user identity using at least two factors before allowing the requested action to be performed.

**Standards:** Several commenters referenced existing standards and guidance that test procedures could be based upon, including:

* DEA Interim Final Rule (IFR)
* NIST 800-63
* FIPS 201
* HSPD-12
* One commenter suggested that ONC could complete a review of the reports sent to the US Federal Public Key Infrastructure (PKI) Policy Authority or the United States Chief Information Officer’s (CIO) Council Federal Identity, Credential, and Access Management (FICAM).

**General Comments:**

* One commenter recommended that attestation be used for how the EHR integrates with two-factor technology.
* One commenter recommends that an iterative and phased testing program is used that covers the population of organizations.
* One commenter recommends that an independent verification of adoption should be conducted as part of attestation.
* One commenter suggests that vendors can select their testing approach, and notes that certification requirements should specify that vendors describe functionality of their solutions fully.
* One commenter notes that vendors could receive certification “credit” if they have implemented a second or third factor mechanism that is listed in NIST 800-63.

**Other:**

* One commenter suggests that EHR certification criteria should include requirements for EHRs to interact with NSTIC Identity Providers during authentication.
* One commenter notes that vendors may act as an identity provider or attribute provider, or they may not. In such circumstances, the testing apparatus would accommodate a network call to the third party identity provider and/or attribute provider to validate the presented credentials and attributes.
* One commenter suggested that the domain is not mature enough for certification.

**Appendix:**

**Test Procedures:** Several commenters made specific suggestions around possible test procedures for the HITPC recommendation in the certification criteria.

* One commenter suggested that the certification criteria be developed following the NSTIC/Identity Ecosystem Accreditation Standards as they are being developed (#14)
* Two commenters suggested use of a checklist or yes/no questions to verify the system set-up, while also requiring for appropriate documentation (#18, #29)
* Two commenters suggested that vendors be required to attest to having an architecture that supports third-party authentication and be capable of demonstrating two examples (#21, #22)
* One commenter suggested that test scenarios should be designed where a subject supplies validated credentials and attribute claims to a relying party who validates the credentials and attributes and performs that transactions requested. (#24)
* One commenter suggested checking for enablement of federation language standard – e.g. SAML, in access and authentication functions, or the ability to accept requests from such a system (#28)
* One commenter suggested the development of a model audit protocol for the community to use to self-test. The commenter notes that stated that control requirements are defined for appropriate audit and credential issuance criteria by 41 CFR Part 11.10. Subpart B (e) and might be considered a basis for developing test objectives in such an audit protocol. (#32)

**Functionality:** Two commenters provided recommendations for specific functionality to be tested as part of the certification criteria.

* Two commenters suggested that EHR technology has the capability to be configured to require two-factor authentication under specified conditions before the user is allowed to perform the requested action (#3,#10)
* Two commenters suggested that EHR technology has the capability to detect the above-mentioned specified conditions and confirm user identity using at least two factors before allowing the requested action to be performed. (#3,#10)

**General Comments:**

* One commenter recommended that attestation be used for how the EHR integrates with two-factor technology (#31)
* One commenter recommends that an iterative and phased testing program is used that covers the population of organizations (#1)
* One commenter recommends that an independent verification of adoption should be conducted as part of attestation (#1)
* One commenter suggests that vendors can select their testing approach, and notes that certification requirements should specify that vendors describe functionality of their solutions fully (#9)
* One commenter notes that vendors could receive certification “credit” if they have implemented a second or third factor mechanism that is listed in NIST 800-63 (#9)

**Standards:** Several commenters reference existing standards and guidance that test procedures could be based upon.

* Standards and guidance referenced by commenters includes: (#4,5,7,8, 27)
	+ DEA Interim Final Rule (IFR)
	+ NIST 800-63
	+ FIPS 201
	+ HSPD-12
	+ One commenter suggested that ONC could complete a review of the reports sent to the US Federal Public Key Infrastructure (PKI) Policy Authority or the United States Chief Information Officer’s (CIO) Council Federal Identity, Credential, and Access Management (FICAM). (#12)

**Other:**

* One commenter suggests that EHR certification criteria should include requirements for EHRs to interact with NSTIC Identity Providers during authentication (#2)
* One commenter notes that vendors may act as an identity provider or attribute provider, or they may not. In such circumstances, the testing apparatus would accommodate a network call to the third party identity provider and/or attribute provider to validate the presented credentials and attributes. (#24)
* One commenter suggested that the domain is not mature enough for certification. (#27)