# PSTT03: Should ONC permit certification of an EHR as stand-alone and/or an EHR along with a third party authentication service provider?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Comment ID |  | 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 “either-or approach” in the degree that each Electronic Health Record (EHR) is certified with each authentication service provider independently.
* Commented that controls between authentication providers cannot be assured and should be treated as separate and unique attributes to the EHR.
 |
| 2 | [HHS-OS-2012-0007-0397](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0397) | p. 12 | Alice Borrelli | Intel Corporation | * No comment.
 |
| 3 | [HHS-OS-2012-0007-0425](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0425) | p. 14 | Willa Fields, Stephen Lieber | HIMSS | * Supported the certification of an EHR that uses third-party security services to meet the required privacy and security requirements.
 |
| 4 | [HHS-OS-2012-0007-0412](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0412) | p. 14 | John Travis | Cerner Corp. | * Stated that certification should allow for an EHR to be certified independently of a third-party authentication service provider.
* Suggested that the criteria should be defined as such where there is a clear separation for the certification of the EHR and the third-party authentication service provider.
* Commented that rigid requirements must be met before an entity can become a provider of authentication services
 |
| 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 | * Commented that third-party authentication services should undergo their own certifications.
* Suggested that use of the third party authentication service should be addressed as part of the risk assessment.
 |
| 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 | * Supported the ANI’s 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 | * Suggested contracting with external labs experienced in testing identity and authentication technologies under the FIPS-201 Evaluation Program.
 |
| 8 | [HHS-OS-2012-0007-0391](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0391) | p. 4 | Karen Boykin-Towns | Pzfizer Inc | * No comment.
 |
| 9 | [HHS-OS-2012-0007-0429](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0429) | p. 7 | Deven McGraw | Center for Democracy and Technology | * Stated that authentication technology used by a third party should be tested in the same way as if it were offered directly by the EHR.
* Suggested that if the efforts to implement National Strategy for Trusted Identities in Cyberspace (NSTIC) result in trusted third-party credentialing processes, potentially those could be relied on in lieu of requiring certification.
 |
| 10 | [HHS-OS-2012-0007-0525](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0525) | p.1 | David Finn | Symantec Corp. | * Supported the certification of an EHR that uses third party services to meet privacy and security requirements.
 |
| 11 | G:\Meaningful Use\HITPC\Stage\_3\_RFC\Submission | p.1 |   | VA | * Invalid link. Cannot 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 | * Suggested that ONC should permit certification of an EHR that uses a third-party authentication service provider affiliated directly or indirectly with the US Federal PKI Architecture or one or more FICAM-approved Trust Frameworks.
* Recommended that the EHR should demonstrate that the credentials it acquires from the third-party provider are either FPKI approved or FICAM approved.
 |
| 13 | [HHS-OS-2012-0007-0210](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0210) | p.11 | Linda  Brady | ADHI | * Supported certification of a standalone EHR and an EHR with third-party authentication service provider should be allowed.
 |
| 14 | [HHS-OS-2012-0007-0325](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0325) | P.12 | Pamela  Foyster | Quality Health Network | * Suggested that this capability be embedded as part of EHR or separate module or add-on.
 |
| 15 | [HHS-OS-2012-0007-0279](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0279) | p.17 | Yomaris  Guerrero | Boston Medical Center | * Supported the ability for ONC to permit the certification of an EHR as stand-alone along with a third-party authentication provider.
 |
| 16 | [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 | * Recommended both types of certification be allowed, as long as the third-party credentialing entity can be certified by an organization designated by the ONC.
 |
| 17 | [HHS-OS-2012-0007-0565](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0565) | p.21 | Leigh  Burchell | Allscripts | * Suggested handling third-party dependencies the same way that database and operating system dependencies are handled in certification today.
 |
| 18 | [HHS-OS-2012-0007-0542](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0542) | p.2-3 | Jim  Williams | Daon | * Believed that there is room for both models.
 |
| 19 | [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 | * Stated that the security requirements should be clearly defined and fully specified in the certification criteria.
* Did not have a preference with regard to the options presented.
 |
| 20 | [HHS-OS-2012-0007-0505](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0505) | p.27 |   | Pharmacy e-HIT Collaborative | * Supported certification with third-party authentication service providers.
 |
| 21 | [HHS-OS-2012-0007-0350](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0350) | p.3 | Landon  Combs | Highlands Physicians Inc | * Expressed agreement with the question, but no recommendation.
 |
| 22 | [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.
 |
| 23 | [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.
 |
| 24 | [HHS-OS-2012-0007-0568](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0568) | p.33 | Sasha  TerMaat | Epic | * Stated that stand-alone certification should be allowed as long as the vendor can demonstrate architecture that allows the use of third-party authentication tools.
 |
| 25 | [HHS-OS-2012-0007-0212](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0212) | p.34 | Kari  Guida | Minnesota Department of Health | * No comment.
 |
| 26 | [HHS-OS-2012-0007-0343](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0343) | p.38 | Donna  Sledziewski | Geisinger Health System | * Stated that certification should permit third-party authentication service providers as long as the provider can demonstrate compliance to standards.
 |
| 27 | [HHS-OS-2012-0007-0332](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0332) | P.4 | Patrick  Sullivan | Harris Corporation | * Supported the adoption of NSTIC Identity Ecosystem Framework. Certification of the third-party authentication service provider.
* Suggested certification should be carried out by an NSTIC Accreditation Authority to a specific healthcare trust framework, which would be recognized by ONC.
 |
| 28 | [HHS-OS-2012-0007-0588](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0588) | p.45 | Gregory  Rivas | UC Davis Medical Center | * Suggested that this may be creating an additional barrier.
* Suggested analysis of how testing of this functionality accomplished today.
 |
| 29 | [HHS-OS-2012-0007-0536](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0536) | p.5 | David  Harlow | Society for Participatory Medicine | * Agreed with question, but offered no recommendation.
 |
| 30 | [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.
 |
| 31 | [HHS-OS-2012-0007-0541](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0541) | p.51 | John  Glaser | Siemens Healthcare | * Stated that it should be permissible to certify the third-party authentication capability separately from the EHR.
 |
| 32 | [HHS-OS-2012-0007-0145](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0145) | p.53 | Nancy  Payne | Allina Health | * Stated that certification should be available for both models.
 |
| 33 | [HHS-OS-2012-0007-0495](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0495) | p.6 |   | Mayo Clinic | * Stated that most large organizations employ institutional identity management schemes and authenticate access at the infrastructure level. Credentials are then passed to the application layer where authorizations are managed, so EHR certification should accommodate this.
 |
| 34 | [HHS-OS-2012-0007-0295](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0295) | p.7 | Susan  Owens | Memorial Healthcare System | * Stated that stand-alone cannot be excluded, because third-party authentication service providers currently are not fully standardized within their own industry; so two different providers may not be able to provide a Federated Account needed to meet NSTICs vision.
 |
| 35 | [HHS-OS-2012-0007-0327](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0327) | P.7 | Megan  Howell | Group Health Cooperative | * Stated that certification of both EHR systems as well as authentication services in a manner similar to the Payment Card Industry (PCI) PA-DSS certification would enable entities to incorporate known secure products and methodologies into their overall compliance strategy.
 |
| 36 | [HHS-OS-2012-0007-0496](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0496) | p.7 | Sara Coulter | Phillips Healthcare | * Stated that ONC should permit certification to include a third-party authentication services provider.
 |
| 37 | [HHS-OS-2012-0007-0476](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0476) | p.8 | Anna Roberts | CHITREC (Chicago Health IT Regional Extension Center) | * Stated that a third-party interface for authentication would be best. This interface could certify independently, then be able to mix and match with all EHRs.
 |
| 38 | [HHS-OS-2012-0007-0520](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0520) | PDF2 - p.78 | Andy Riedel | NextGen Healthcare | * Stated that this approach will likely be the appropriate one in many cases, as two-factor technologies are not core EHR competencies.
* Suggested handling third-party dependencies the same way that database and operating system dependencies are handled in certification today.
 |
| 39 | [HHS-OS-2012-0007-0547](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0547) | tab 3 | Erin  Laney | Intermountain Healthcare | * Suggested that ONC consider establishing standards for what assurance level third-party authentication services must provide.
 |
| 40 | [HHS-OS-2012-0007-0535](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0535) | tab 4 | Dan  Rode | American Health Information Management Association | * Stated that both the EHR as a stand-alone and the EHR along with the third-party authentication service provider should be certified. This will allow more flexibility.
 |

**Summary**

**Number of Comments: 30** (10 commenters did not include a response or link was invalid)

**Summary:**

Commenters included those in favor of permitting certification of an EHR that uses third party authentication services, those in favor of permitting certification of the EHR and third party authentication service providers independently, and those in favor of certification for both models. A few commenters proposed alternate methods to certification for third party authentication services.

* A number of commenters believe that ONC should permit certification of an EHR that uses third party authentication services. (10)
	+ One commenter noted that the authentication provider should be affiliated directly or indirectly with the US Federal PKI Architecture or one or more FICAM approved Trust Frameworks.
* A number of commenters believe that ONC should permit certification of the EHR and the third party authentication service providers independently. (6)
* A number of commenters believe that both types of certification should be permitted. (4)
* Two commenters suggested handling third party dependencies the same way that database and operating system dependencies are handled in certification today.
* Two commenters noted that in lieu of requiring certification ONC could implement NSTIC which would result in a trusted third-party credentialing process.
	+ One commenter noted that certification could be carried out by a NSTIC Accreditation Authority to a specific healthcare trust framework, which would be recognized by ONC.
* One commenter noted that authentication services implemented in a similar way to the Payment Card Industry (PCI) PA-DSS certification would enable entities to incorporate known secure products and methodologies into their overall compliance strategy.
* One commenter noted that third party authentication service could be addressed as part of the risk analysis.
* One commenter believes that contracting with external labs experienced in testing identity and authentication technologies under FIPS 201 Evaluation Program for third party authentication providers.

**Appendix:**

Commenters included those in favor of permitting certification of an EHR that uses third party authentication services, those in favor of permitting certification of the EHR and third party authentication service providers independently, and those in favor of certification for both models. A few commenters proposed alternate methods to certification for third party authentication services.

* A number of commenters believe that ONC should permit certification of an EHR that uses third party authentication services. (#3, #10, #13, #14, #15, #16, #20, #24, #34, #36)
	+ One commenter noted that the authentication provider should be affiliated directly or indirectly with the US Federal PKI Architecture or one or more FICAM approved Trust Frameworks. (#12)
* A number of commenters believe that ONC should permit certification of the EHR and the third party authentication service providers independently. (#1, #4, #5, #31, #35, #37)
* A number of commenters believe that both types of certification should be permitted. (#16, #18, #32, #40)
* Two commenters suggested handling third party dependencies the same way that database and operating system dependencies are handled in certification today. (#21, #38)
* Two commenters noted that in lieu of requiring certification ONC could implement NSTIC which would result in a trusted third-party credentialing process. (#9, #27)
	+ One commenter noted that certification could be carried out by a NSTIC Accreditation Authority to a specific healthcare trust framework, which would be recognized by ONC. (#27)
* One commenter noted that authentication services implemented in a similar way to the Payment Card Industry (PCI) PA-DSS certification would enable entities to incorporate known secure products and methodologies into their overall compliance strategy. (#35)
* One commenter noted that third party authentication service could be addressed as part of the risk analysis. (#5)
* One commenter believes that contracting with external labs experienced in testing identity and authentication technologies under FIPS 201 Evaluation Program for third party authentication providers. (#7)