**Federal Register**/Vol. 79, No. 38/Wednesday, February 26, 2014/Proposed Rules

**V. Other Topics for Consideration for the 2017 Edition Certification Criteria Rulemaking**

**…**

*C. Certification Policy for EHR Modules and Privacy and Security Certification Criteria* [pp. 10925-10926]

In our past rulemakings we have discussed and instituted two different policy approaches for ensuring that EHR Modules meet privacy and security (P&S) certification criteria while minimizing the level of regulatory burden imposed on EHR technology developers. In the 2011 Edition, we required that EHR Modules must meet all P&S certification criteria unless the presenter could demonstrate that certain P&S capabilities were either technically infeasible or inapplicable. In the 2014 Edition, we eliminated the requirement for each EHR Module to be certified against the P&S criteria. Rather, the P&S criteria were made part of the ‘‘Base EHR definition’’ that all EPs, EHs, and CAHs must have EHR technology certified to meet, in order to ultimately have EHR technology that satisfied the CEHRT definition. While some commenters expressed concern with our 2014 Edition proposal to remove the P&S certification requirement for EHR Modules, we finalized the policy in favor of the outcome-oriented requirement we believed the Base EHR definition promoted, and in an effort to enable EHR technology developers to better choose which P&S criteria were most applicable to their products. As of December 31, 2013, approximately 70% of 2014 Edition EHR Modules have been certified to at least one P&S criterion (out of nine available P&S criteria) and about 51% have been certified to four or more. Despite prior stakeholder concerns, this data suggests that our 2014 Edition Final Rule policy has not resulted in a significant reduction in the number of EHR Modules certified to P&S criteria and that a majority of EHR technology developers appear to be pursuing certification to these criteria regardless of our more flexible, less burdensome policy for 2014 Edition certification.

|  |
| --- |
| DBaker NOTE: The nine 2014 Edition Privacy and Security certification criteria are:   1. *Authentication, access control, and* *authorization.* 2. *Auditable events and tamper- resistance.* 3. *Audit report(s).* 4. *Amendments.* 5. *Automatic log-off.* 6. *Emergency access.* 7. *End-user device encryption.* 8. *Integrity.* 9. *Optional - Accounting of disclosures.* |

On March 23, 2013, the HITSC recommended that we should change our EHR Module certification policy for P&S. They recommended that each EHR Module presented for certification should be certified through one or more of the following three paths:

* Demonstrate, through system documentation and certification testing, that the EHR Module includes functionality that meets at least the ‘‘minimal set’’ 127 of privacy and security certification criterion.

127 The minimal set includes Authentication, access control, and authorization, Auditable events and tamper resistance, Audit report(s), Amendments, Automatic log-off, Emergency access, End-user device encryption, and Integrity. The full recommendation can be found at: *http:// www.healthit.gov/sites/default/files/pswg transmittalmemo**032613.pdf*.

* Demonstrate, through system documentation sufficiently detailed to enable integration, that the EHR Module has implemented service interfaces that enable it to access external services necessary to conform to the ‘‘minimal set’’ of privacy and security certification criterion.
* Demonstrate through documentation that the privacy and security certification criterion (and the minimal set that the HITSC defined) is inapplicable or would be technically infeasible for the EHR Module to meet. In support of this path, the HITSC recommended that ONC develop guidance on the documentation required to justify inapplicability or infeasibility.

As a result of the HITSC recommendations and stakeholder feedback, we seek comment on the following four options we believe could be applied to EHR Module certification for privacy and security:

* *Option 1:* Re-Adopt the 2011 Edition approach.
* *Option 2:* Maintain the 2014 Edition approach.
* *Option 3:* Adopt the HITSC recommendation. This approach reintroduces some of the challenges we sought to avoid with our current policy and introduces potentially new administrative burdens for EHR technology developers.
* *Option 4:* Adopt a limited applicability approach—under this approach, ONC would establish a limited set of P&S functionality that every EHR Module would be required to address in order to be certified. For example, we could require that all EHR Modules need to address the authentication, access control, and authorization certification criterion. This approach has the same downsides as options 1 and 3 but to a lesser extent given that its broad applicability could still result in EPs, EHs, and CAHs adopting EHR Modules that had been certified with duplicative capabilities.

We seek feedback on all of these policy options. Further we especially solicit feedback: (1) from EHR technology developers and ONC–ACBs regarding the efficiency of the current certification policy; (2) from stakeholders that prefer ‘‘option 3’’ (the HITSC’s recommendation) and why; and (3) from stakeholders that prefer ‘‘option 4’’ what the minimum P&S criteria could be.

**Proposed EHR Module Certification Change for 2015-2017**

**§ 170.550 EHR Module certification.**

\* \* \* \*

(e) [Reserved]

(f) When certifying an EHR Module to the 2014 Edition EHR certification criteria, an ONC–ACB must certify the EHR Module in accordance with the certification criteria at:

(1) Section 170.314(g)(1) or (g)(2) if the EHR Module has capabilities presented for certification that would support a meaningful use objective with a percentage-based measure;

\* \* \* \* \*

 (g) When certifying an EHR Module to the 2015 Edition EHR certification criteria, an ONC–ACB must certify the EHR Module in accordance with the certification criteria at:

(1) Section 170.315(g)(1) or (g)(2) if the MU EHR Module has capabilities presented for certification that would support a meaningful use objective with a percentage-based measure;

(2) Section 170.315(g)(3) if the EHR Module is presented for certification to one or more listed certification criteria in § 170.315(g)(3);

(3) Section 170.315(g)(4); and

(4) Section 170.315(g)(5) if the MU EHR Module has capabilities presented for certification that would support a meaningful use objective with a non- percentage-based measure.

\* \* \* \* \*