Health IT Standards Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

Privacy & Security Workgroup - 2015 NPRM Comments

Dixie Baker, Chair
Lisa Gallagher, Co-Chair

April 24, 2014

PSWG Members

- Dixie B. Baker, Chair, Martin, Blanck, and Associates
- Lisa Gallagher, Co-Chair, HIMSS
- A. John Blair, III, Member, Taconic IPA
- Mike Davis, Member, Department of Veterans Affairs
- Leslie Kelly-Hall, Member, Healthwise
- Chad Hirsch, Member, Mayo Clinic
- Peter Kaufman, Member, DrFirst
- Ed Larsen, Member, HITSP
- David McCallie, Jr., Member, Cerner Corporation
- John Moehrke, Member, General Electric
- Sharon F. Terry, Member Genetic Alliance

Topics

PSWG Comments (comment source)	ONC Comment Request	2015 Edition Issues	2017 Edition Issues	Changes from 2014 Final Rule to 2015 NPRM/ONC Requests
Module Certification against Privacy and Security Criteria (ONC NPRM team requested PSWG feedback)	X		X	ONC requests feedback on approaches for certifying the privacy and security of EHR modules; options include 2011 approach, 2014 approach, HITSC-recommended approach, and subsetting approach
Authentication, Access Control, Authorization (assigned by HITSC)	X		X	ONC requests feedback on 2-factor authentication for two use cases re: 2017 NPRM.
Auditable Events and Tamper Resistance (assigned by HITSC)	X	X		The 2014 Final Rule allows for selected users to disable audit logging and the 2015 proposal is to remove this functionality. ONC is looking for feedback re: this proposal.
Audit Report(s) (assigned by HITSC)	X		X	ONC is not proposing changes but wants feedback on the use of ASTM E1247 re: 2017 NPRM.
Accounting of Disclosures (assigned by HITSC)	X			ONC proposing removal of optional status in light of changes to the definition of "complete EHR". No discussion of HIPAA rule in 2015 NPRM.
Blue Button+ (PSWG initiated)	X		X	Potential certification criterion for 2017.
Disaster Preparedness (PSWG initiated)	X		X	Potential certification criterion for 2017.

EHR Module Certification Against Privacy and Security Criteria (1 of 6)

NPRM Request (for 2017)

- Seeks comment on four options for certifying EHR Modules for privacy and security:
  - *Option 1:* Re-Adopt the 2011 Edition approach (certify all EHR Modules against all P&S criteria)
  - *Option 2:* Maintain the 2014 Edition approach (certify EHR Modules against P&S criteria only at vendor's request)
  - *Option 3:* Adopt the HITSC recommendation – (certify all EHR Modules against all P&S criteria, via any one of three paths)
  - *Option 4:* Adopt a limited applicability approach
    - Establish a limited set of P&S functionality that every EHR Module would be required to address in order to be certified

EHR Module Certification Against Privacy and Security Criteria (2 of 6)

HITSC Recommendation, transmitted to ONC March 23, 2013

- For 2016 Edition EHR certification, each EHR Module presented for certification should be required to meet each privacy and security criterion using one of the following three paths:
  1. Demonstrate, through system documentation and certification testing, that the EHR Module includes functionality that fully conforms to the privacy and security certification criterion.
  2. 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 privacy and security certification criterion.
  3. Demonstrate through documentation that the privacy and security certification criterion is inapplicable or would be technically infeasible for the EHR Module to meet.

EHR Module Certification Against Privacy and Security Criteria (3 of 6)

PSWG Response

We agree that having each EHR Module implement its own security solution (2011 approach) is not ideal; for strongest security protection, each EHR Module would use a common set of enterprise-wide security services. Path 2 of the HITSC's 2013 recommendation recognizes this ideal. The 2014 approach (certifying EHR Modules privacy and security only at the vendor's request) presents the risk that an end user could purchase a set of modules that would not provide the protection needed to counter risks present in that environment. However, we recognize that the privacy and security criteria are not equally applicable or useful to every criterion in each of the other functional areas (i.e., clinical, care coordination, clinical quality, patient engagement, public health, utilization) because each P&S criterion is designed to address specific risk conditions that may or may not be present.

EHR Module Certification Against Privacy and Security Criteria (4 of 6)

PSWG Response (cont.)

We therefore recommend that ONC:

1) Revise each privacy and security criterion to specify the conditions under which it is applicable (similar to how the end-user device encryption criterion currently is written) AND
2) Allow each criterion to be met using one of the three paths the HITSC recommended in 2013.

This can be accomplished by modifying the wording of the criteria in the regulation to include the condition(s), or by providing the condition(s) as guidance. In either case, the condition(s) and paths would need to be incorporated into test procedure. If this approach is accepted, the PSWG would be happy to work with ONC to help with the implementation.

EHR Module Certification Against Privacy and Security Criteria (5 of 6)

Example #1:

The *current* **end-user device encryption** criterion provides a good example of the proposed approach as worded in the regulation**:**

(7) *End-user device encryption.* Paragraph (d)(7)(i) or (ii) of this section must be met to satisfy this certification criterion.

(i) EHR technology ***that is designed to locally store electronic health information on end-user devices*** must encrypt the electronic health information stored on such devices after use of EHR technology on those devices stops.

EHR Module Certification Against Privacy and Security Criteria (6 of 6)

Example #2:

Criterion, as currently worded:

Emergency Access: Permit an identified set of users to access electronic health information during an emergency.

Applicability Statement:

If the module allows human users access to electronic health information, *and*

If the module performs functions supporting the purpose of delivering patient care,

demonstrate how the module supports emergency access by an identified set of users.

Authentication, Access Control, and Authorization (1 of 2)

NPRM Request (for 2017)

ONC is requesting comment on two-factor authentication in reference to two use cases:

- e-prescribing of controlled substances
- remote provider access to EHR technology

Specifically:

1) Whether the HIT Policy Committee's recommendations are appropriate and actionable and, if not, what level of assurance should be the minimum required for provider-users seeking remote access to EHR technology."

2) Whether we should adopt a general two-factor authentication capability requirement for certification…[which] could complement e-prescribing of controlled substances requirements and more definitively support security requirements for remote access to EHR technology as well as any other EHR technology uses that may require two factor authentication."

Authentication, Access Control, and Authorization (2 of 2)

PSWG Response (2017)

1) **Re: appropriateness and actionability of HITPC recommendation:**
The HITPC's policy recommendations are actionable, as the capability to require two forms of authentication can be tested functionally (for example, using the 800-63-2 LOA 3 functional specification). However, given the number of approaches that can be used in two-factor authentication for remote access, and the fact that authentication technology is likely to advance over the next three years, the PSWG cannot recommend a specific set of standards to use for this purpose.

2) **Re: broad adoption of two-factor authentication:**
We are not aware of any meaningful-use measures or other healthcare policy that would warrant a general requirement for a two-factor authentication capability. However, if the ONC decides to add such a requirement, the PSWG suggests that a product presenting proof of having passed a DEA audit of its two-factor authentication capability should be considered as having met the certification requirement for two-factor authentication for an EHR, but not necessarily for remote access. We would again note that this can only be tested functionally (see response above). The PSWG also would observe that these two use cases (e-prescribing of controlled substances and remote access) highlight the need for healthcare engagement with the NSTIC program.

Auditable Events and Tamper Resistance (1 of 2)

NPRM Request

The 2014 Final Rule allows for selected users to disable audit logging, and the 2015 proposal proposes to remove this functionality. ONC seeks comment on the "impact and potential unintended consequences of" their proposed change "and specific examples where disabling an EHR technology’s audit log is warranted.”

Auditable Events and Tamper Resistance (2 of 2)

PSWG Response

The PSWG suggests no change from the 2014 Final Rule; the current criteria adequately function as a floor for meaningful use.

Although the current certification criteria do not preclude the audit log from being disabled, they do require access controls restricting the capability to disable the audit log to a limited set of identified users (presumably those with audit-log administrative duties) and the capability to record the user ID, data, and time when the log was disabled. Since the proposed change would "prevent all users from disabling the audit log," the PSWG contends that prohibiting the disabling of the audit log would hamper security administrators from performing their functions properly.

Generally, this kind of action comes from concern that a system administrator would do something nefarious. A countermeasure is to audit the act of turning the audit log off and on; this capability is required in the current criteria. Furthermore, audit administrators are typically separate from other security administrators. Audit administration typically includes tuning (disabling) the list of audited events or turning off positive authentication events while leaving negative authentication events enabled. Sometimes, the storage capacity required for the audit trail expands and can threaten continuing operations. While the PSWG does not suggest a regular practice of disabling the audit trail to manage storage, it does suggest that certification criteria should not thwart administrators ability to perform their assigned functions.

Audit Report(s) (1 of 3)

NPRM Request (for 2017)

ONC is requesting comments on the sufficiency of ASTM E1247 for the 2017 NPRM, specifically:

1) "The 'query' action in section 7.6 of the ASTM E2147 standard is not a defined term in the standard’s definition section." ONC wants to know A) "whether this ambiguity has caused additional burden or challenges for EHR technology developers," B) "how EHR technology developers have interpreted the term when designing their EHR technology," and C) if there is any "industry knowledge related to any plans to revise ASTM E2147 to address this ambiguity.“

2) "Whether [ONC] should establish a minimum/baseline set of actions that EHR technology must always be capable of" for the purpose of audit?

3) Whether there are other actions that ONC should consider specifying in an updated standard for the 2017 Edition that the current standard does not sufficiently address, such as the act of ‘transmission’? ONC does not favor this approach because implementing it in regulation would cause addition to the existing standard and seeks feedback on whether the standard is sufficiently up-to-date and appropriately specifies all of the actions necessary for EHR audit logs to capture.

4) Are there "any alternative standards to ASTM E2147 that [ONC] should consider in light of the aforementioned concerns and ambiguities.”

Audit Report(s) (2 of 3)

PSWG Response (2017)

1) **Re: The 'query' action in section 7.6 of the ASTM E2147 standard:**
ASTM E2147 was updated a year ago, and the PSWG is not aware of any need to define ‘query’ or any problems developers have encountered regarding query. Greater vendor input is needed to fully answer this question for the entire healthcare industry. We recognize that there is confusion in the market in understanding the Security Audit Logging concept. We would suggest that a broader reference to ASTM E2147 might serve well to help clarify any misunderstandings. Specifically, we recommend expanding the references to include at least section 5 which explains Security Audit Logging and describes the kinds of events that should be recorded in the audit log. In addition, we recommend that Section 7 be referenced in its entirety, rather than individually enumerating those parts of Section 7 that are not labeled “optional.” Note that by citing all of Section 7, the labeled provisions still would be treated as “optional.”

2) **Re: Minimum/baseline set of actions for the purpose of audit**
Typically, one audits security-relevant actions associated with performing required functions; one does not require functions so that they can be audited. The PSWG is opposed to establishing a minimum or baseline set of actions that EHR technology must always be capable of so that they can be audited.

Audit Report(s) (3 of 3)

PSWG Response (2017)

3) **Re: Other actions to consider specifying, such as the act of ‘transmission’:**
The PSWG believes it is quite feasible to certify EHR compliance with the ASTM E2147 audit log standard, and does not recommend ONC specify other actions in an updated standard for the 2017 Edition, or that ONC consider any additional standards.

4) **Re: Alternative standards to consider:**
The PSWG believes it is quite feasible to certify EHR compliance with the ASTM E2147 audit log standard, and does not recommend that ONC consider any additional standards.

Accounting of Disclosures

NPRM Request

ONC plans "to adopt 2015 Edition certification criterion that is the same text as the 2014 Edition version. However, given [ONC's] proposal to discontinue the Complete EHR concept" ONC is proposing that this criterion no longer be optional as "such a designation would no longer be necessary."

PSWG Response

Since OCR has not yet issued its final rule, the PSWG believes it is premature to include an Accounting of Disclosures criterion at this time.

Blue Button +

NPRM Request (for 2017)

The NPRM specifically solicits comments on the following questions :

1) "Is there a market need for BB+ certification? In other words, would health IT developers find value in a BB+ certification that would enable them to say they are "BB+ compliant" or "BB+ ready";

2) Which elements of BB+ Direct Specifications would be most important to reference in a certification criterion and how would they be tested; and

3) What elements of BB+ REST Specifications would be most important to reference in a certification criterion and how would they be tested? Additionally, what use cases would be uniquely supported by BB + REST Specifications?" (2015 NPRM, p. 173-174)

PSWG Response

PSWG encourages and supports further piloting, direction, and standards development for Blue Button Plus (BB+). However, PSWG feels that at this point, prescribing specific standards that BB+ must use could potentially constrain the momentum surrounding its technological advancement.

Disaster Preparedness (1 of 2)

NPRM Request (for 2017)

The NPRM solicits comments on the following questions related to disaster preparedness/emergency situations:

1) Whether there could be a standardized naming convention for EHR technology to use for temporarily naming unidentified patients during disaster and emergency events?

2) Whether we should consider adopting a certification criterion that would be available for certification for EHR technology developers to show that their EHR technology can batch print face sheets or patient snapshots in bulk (by floor or unit, or by facility) to support movement/evacuation of large numbers of patients?

3) Whether there are particular capabilities or standards we should consider as part of EHR certification that would better assist providers track and identify patients and victims and share basic clinical information quickly across the full continuum of care during everyday emergencies, disasters, and public health emergencies?

4) Whether EHR technology should be able to denote care provided during disasters or public health emergencies and allow for designation of care provided under situations which demand contingency or crisis standards of care?

5) Whether there are any EHR capabilities and certification criteria that we should consider for certification that could improve/expedite how EHR technology is used to report standardized and de-identified patient data to public health and emergency management authorities, in a manner that would allow such authorities the ability to measure, track and trend health system resiliency, stress, preparedness, and recovery?”

Disaster Preparedness (2 of 2)

PSWG Response (2017)

PSWG believes that ONC's solicitation for comment on standards related to disaster preparedness is premature, as there are unresolved policy questions that must be answered prior to any attempt to determine what standards EHR technology should use to support the provision of care in disaster situations.