

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

Updates from April 24, 2014 HITSC meeting

Dixie Baker, Chair
Lisa Gallagher, Co-Chair

June 17, 2014



- 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
- Walter Suarez, Kaiser Permanente
- Sharon F. Terry, Member, Genetic Alliance



- HITSC Comments/PSWG revised responses
 - Two-Factor Authentication
 - Accounting of Disclosures
 - Audit clarification within the context of ASTM E2147
- PSWG proposed wording edits
 - Server authentication
 - Automatic time-outs

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



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

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)



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

PSWG Response (2017)

1) **Re: appropriateness and actionability of HITPC recommendation:**

The HITPC's policy recommendations are actionable, from a certification perspective, 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.

However, from a policy perspective, we would note that in today's environment, "remote access" may be difficult to define, as it is situational. For example, would EHR access using a mobile device within a hospital be considered "remote access?" Given this difficulty, the PSWG concludes that the level of assurance required for provider-users seeking remote access to EHR technology should be based on an assessment of the relative risk associated with the particular access approach used.

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.



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

The PSWG agrees with ONC’s recommendation to remove the “optional” designation associated with the accounting of disclosures criterion. With the elimination of the complete EHR concept, such a designation no longer is necessary.



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."



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**

Section 7.6 of ASTM E2147 specifies the types of actions to be included in the audit trail and should cover any type of action taken within an enterprise. In response to ONC's question regarding the inclusion of "transmission" as an action, the PSWG concluded that transmitting a record within an enterprise would require a "copy" and thus, is already addressed in section 7.6.



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.



- “Applicability specifications” exercise (see April 24, 2014, recommendations) uncovered several criteria in 2014 that could be improved
 - Authentication addresses people, not software
 - Automatic logoff does not include preliminary step of automatic screen-lock

Proposed Language Modifications – Server Authentication and Time-outs



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

- **Server authentication** – Re § 170.315(d)(1) (*Authentication, Access Control, and Authorization*) (i) *Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed*
 - The PSWG also notes the need for authentication to extend beyond persons to software application or servers and recommends modifying the above language to include servers seeking access to electronic health information, for example: (i) *Verify against a unique identifier(s) (e.g., username or number) that a person **or software application or server** seeking access to electronic health information is the one claimed;*
- **Automatic time-outs** – Re § 170.315(d)(5) (*Automatic log-off*) *Prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.*
 - In common practice, end-user device screens are timed out (e.g., “lock screen”) after an initial period of inactivity, rather than terminating the session altogether. The PSWG therefore suggests refining this criterion as follows: (5) *Automatic time-out and log-off.* *Automatically block access to PHI until the original user re-authenticates or another authorized user authenticates; automatically log-off the user after a (longer) sustained, predetermined period of inactivity.*