Transport and Security Standards (TSS) Workgroup

Certification NPRM Comment Template

Proposed 2015 Edition Electronic Health Record (EHR) Certification Criteria, 2015 Edition Base EHR Definition, and ONC Health IT Certification Program Modifications

C. Health IT Module Certification Requirements pp. 258-261 & Appendix A (Public Inspection Version Numbering)[1]	
Preamble FR Citation: 80 FR 16875	**Specific questions in preamble?** *Yes*

Public Comment Field:

The HITSC Transport and Security Standards Workgroup (TSSWG) members agree that the new approach for privacy and security (P&S) certification in the 2015 Edition is a step in the right direction and is generally both clear and feasible. ONC's proposal for P&S mostly aligns with past Workgroup recommendations, but we are recommending a few modifications. Specifically, the TSSWG recommends adding the **following P&S criteria**:

- Clinical Module (§ 710.315(a)): We initially interpreted the exclusion of the Integrity criterion (§ 710.315(d)(8)) as an oversight. However, at the April 2015 HITSC meeting, ONC explained that this was not the case, and that the thinking was that because the data integrity criterion relates to transmitted data, and the clinical criteria do not involve transmissions, the integrity criterion should not apply. We would point out that the Clinical criteria do include the following criteria that involve transmissions: "(ii) Technology must be able to receive and incorporate a new or updated laboratory order compendium…" and "(vi)(C) Receive and incorporate a formulary and benefit file…." Depending upon the module architecture, other clinical criteria may involve transmissions as well. In addition, we would note that message digests are used to protect the integrity of other content besides transmissions, including digital signatures and secure electronic mail. We therefore recommend that the Integrity criterion (§ 710.315(d)(8)) NOT be excluded from applicability to Clinical modules. Data integrity ensures the accuracy of clinical information, which is a vital patient safety imperative. Therefore, **we recommend that ONC add the Integrity certification criterion to the list of Security criteria against which a Clinical Module must be certified**.
- Care Coordination Module (§ 710.315(b)): **The TSSWG recommends adding the Amendments criterion (§ 710.315(d)(4)) to the list of security criteria against which a Care Coordination Module is certified**. This Module should support patient requested amendments to electronic health information maintained in an electronic health record (EHR).
- Design and Performance Module (§ 710.315(g)): We agree that the Security and Privacy criteria are not applicable to most of the Design and Performance criteria. The only exception is (g)(7) Application Access to Common Clinical Data Set. **We recommend that the following Privacy and Security criteria be applied to the API criterion**: (**1) Authentication, access control, and authorization; (2) Auditable events and tamper resistance; and (8) Integrity**.

The TSSWG believes the proposed approach to P&S in the 2015 Edition is helpful from a vendor perspective because vendors will have a clear and succinct reference to a matrix, which includes paragraph references to what would be required to meet certification. The Workgroup anticipates the potential for some initial resistance to adoption, especially depending on current vendor product capabilities and provider investments. Nevertheless, the proposed changes to P&S certification – including the modifications suggested above – are an important and appropriate advance.

[1] See Public Inspection Document, available at: https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-06612.pdf.

§ 170.315(d)(2) Auditable events and tamper-resistance pp. 151-154 (Public Inspection Version Numbering)	
Included in 2015 Edition Base EHR Definition? No, but a conditional certification requirement	
MU Objective N/A	
2015 Edition Health IT Certification Criterion (2) Auditable events and tamper-resistance. (i) Record actions. Technology must be able to: (A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1); (B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and (C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section). (ii) Default setting. Technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraph (d)(2)(i)(B) or (C) of this section, or both paragraphs (d)(2)(i)(B) and (C). (iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users. (iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the technology. (v) Detection. Technology must be able to detect whether the audit log has been altered.	
Preamble FR Citation: 80 FR 16846	**Specific questions in preamble?** *Yes*

Public Comment Field:

The ONC has asked the TSSWG (and the Privacy and Security Workgroup that preceded it) for recommendations about auditable events as part of several NPRM reviews. We have responded to each query independently, but have not previously noticed the primary omission that perhaps has given rise to these questions – the current Certification Criteria and Standards **lack a certification criterion stating what events need to be recorded in an audit trail.**

The only standard cited for the "Auditable events and tamper resistance" criteria is ASTM E2147-01, *Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems,* Section 5 of which addresses "events" to be audited, with Section 7 specifying the data elements that need to be included for each auditable event. Unfortunately ASTM E2147-01 addresses only events relating to accesses to health information, not the broad category of "security-relevant events" that need to be included in an audit trail.

The TSSWG investigated potential standards that could be used to capture the full purpose and need for auditing, and concluded that NIST SP 800-92 (http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf), *Guide to Computer Security Log Management*, will serve this purpose nicely. **We recommend that § 170.315(d)(2)(i)(A) be revised to read**:

> (2) Auditable events and tamper-resistance--(i) Record security-relevant events. Technology must be able to (A) Record the data elements specified in section 7 of § 170.210(e)(1) for all security-relevant events performed by the HIT, including (1) events identified in [new standard: NIST SP 800-92, Sections 2.1.2-2.1.3] and (2) events related to accesses to electronic health information as specified in section 7 of § 170.210(e)(1);

This change is responsive to ONC's question asking **whether a change in user privileges needs to be auditable** – the TSSWG's answer is **"yes" because a change in user privilege is a security-critical event**.

Additionally, the TSSWG would direct ONC to a list of security-relevant events set forth by the non-profit Open Web Application Security Project (OWASP). The OWASP list is not a standard, but is offered as a helpful reference for ONC as it considers which security-related events should be auditable. The list is available at: https://www.owasp.org/index.php/Logging_Cheat_Sheet#Which_events_to_log.

The TSSWG would further note that while certified HIT should be required to be "capable of recording an audit trail of" security-relevant events, the determination of which auditable events should actually be "audited" is a risk management decision that should be made by security professionals of each implementing organization.

As to the question of whether a critical subset of events should never be disabled, the TSSWG agrees with the previous recommendations on auditable events and tamper-resistance from April 2014 (available at: http://healthit.gov/archive/archive_files/HIT%20Standards%20Committee/2014/2014-04-24/HITSC_PSWG_2015NPRM_Final_2014-04-24.pdf) and **recommends no change from the 2014 Final Rule, which permits audit logs to be temporarily disabled**. For the reasons stated in previous recommendations, the current criteria adequately function as a floor for meaningful use.

§ 170.315(d)(5) Automatic access time-out pp. 155-156 (Public Inspection Version Numbering)	
Included in 2015 Edition Base EHR Definition? No, but a conditional certification requirement	
Stage 3 MU Objective N/A	
2015 Edition Health IT Certification Criterion (5) Automatic access time-out. (i) Automatically stop user access to health information after a predetermined period of inactivity. (ii) Require user authentication in order to resume or regain the access that was stopped.	
Preamble FR Citation: 80 FR 16847	**Specific questions in preamble?** *Yes*

Public Comment Field:

The TSSWG recommends changing the language from: "(i) Automatically stop user access to health information after a predetermined period of inactivity" to "**Automatically terminate access to protected health information after a system- and/or administrator-defined period of inactivity, and reinitiate session upon re-authentication of the user**".

§ 170.315(d)(7) End-user device encryption pp. 157-158 (Public Inspection Version Numbering)	
Included in 2015 Edition Base EHR Definition? No, but a conditional certification requirement	
Stage 3 MU Objective N/A	
2015 Edition Health IT Certification Criterion (7) End-user device encryption. Paragraph (d)(7)(i) or (ii) of this section must be met to satisfy this certification criterion. (i) 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 the technology on those devices stops. (A) Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(3). (B) Default setting. Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users. (ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.	
Preamble FR Citation: 80 FR 16847	**Specific questions in preamble?** *Yes*

Public Comment Field:

The TSSWG supports the NPRM proposal to update the encryption standard to the October 2014 release of FIPS 140-2, Annex A.

In addition, **we recommend adding a reference to the FIPS 140-2, Annex A, guideline for Transport Layer Security (TLS) to support the proposed new certification criteria for "application access" for Patient Engagement** [170.315(e)(1)(iii)] **and for accessing the**

Common Clinical Data Set [170.315(g)(7)]. Specifically, the Workgroup recommends adding references to the TLS guideline referenced in FIPS 140-2, Annex A, for securing channels to the exposed service endpoints:

- Page 16905 in Fed. Reg., para. 170.210, add a reference to *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* recommended in FIPS 14002, Annex A.
- Page 16912 in Fed. Reg., para. 170.315(e)(1)(iii)(A), incorporate into security criterion for Application Access for Patient Engagement.
- Page 16193 in Fed. Reg., para. 170.315(g)(7)(i), incorporate into security criterion for Application Access to Common Clinical Data set.

§ 170.315(d)(8) Integrity pp. 157-158 (Public Inspection Version Numbering)	
Included in 2015 Edition Base EHR Definition? No, but a conditional certification requirement	
Stage 3 MU Objective N/A	
2015 Edition Health IT Certification Criterion (8) Integrity. (i) Create a message digest in accordance with the standard specified in § 170.210(c). (ii) Verify in accordance with the standard specified in § 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered.	
Preamble FR Citation: 80 FR 16847	**Specific questions in preamble?** *Yes*

Public Comment Field:

The Workgroup members agree with ONC's proposal to move to SHA-2 in the 2015 Edition.

§ 170.315(b)(7) Data segmentation for privacy – send pp. 135-136 (Public Inspection Version Numbering) **§ 170.315(b)(8) Data segmentation for privacy – receive pp.135-136**	
Included in 2015 Edition Base EHR Definition? No	
Stage 3 MU Objective N/A	
2015 Edition Health IT Certification Criterion (7) Data segmentation for privacy – send. Technology must enable a user to create a summary record formatted in accordance with each of the standards adopted in § 170.205(a)(3) and (4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1). (8) Data segmentation for privacy – receive. Technology must enable a user to: (i) Receive a summary record that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1); (ii) Apply document-level tagging and sequester the document from other documents received; and (iii) View the restricted document (or data), without incorporating the document (or data).	
Preamble FR Citation: 80 FR 16841 and 16842 (also see 80 FR 16840)	**Specific questions in preamble?** *No*

Public Comment Field:

The TSSWG shares ONC's concern that sensitive health information is not typically kept in the same repositories as non-sensitive health information and is often excluded from electronic health information exchange (eHIE). The TSSWG agrees that establishing nationwide standards for sharing sensitive health information is a critically important step towards improving both health IT interoperability and patient health outcomes. However, the **TSSWG's assessment is** that **the Data Segmentation for Privacy (DS4P) technology is not ready to become a national standard for certifying HIT**.

The TSSWG acknowledges the pilot implementations of DS4P under the sponsorship of the Substance Abuse and Mental Health Administration (SAMHSA) and the U.S. Department of Veterans Affairs (VA), but adoption beyond these pilots is only beginning, and large vendors are just now experimenting with DS4P implementation. Based on the readiness criteria developed and adopted by the HITSC, the TSSWG concludes that DS4P is not yet ready to be adopted as a national standard.

In sum, given that the DS4P standard requires additional pilots and more widespread adoption to answer critical questions, the **Workgroup concludes that DS4P is not sufficiently mature to be promoted in law as a national standard, and the Workgroup recommends that ONC not include DS4P Send and Receive as voluntary criteria in the 2015 Edition**. Because the Workgroup strongly believes that technologies like DS4P are important for the future of health IT interoperability and patient outcomes, **the Workgroup urges ONC to collaborate with other stakeholders within government and industry to identify and employ other levers and methods to promote more widespread adoption of DS4P**.

§ 170.315(i)(1) Electronic submission of medical documentation pp. 222-234 (Public Inspection Version Numbering)

Included in 2015 Edition Base EHR Definition?

No

Stage 3 MU Objective

N/A

2015 Edition Health IT Certification Criterion

(1) Electronic submission of medical documentation.

(i) Document templates. Health IT must be able to create electronic documents for transmission formatted according to the following standard and applicable implementation specifications adopted at § 170.205(a)(4) and (a)(5)(i). With respect to § 170.205(a)(5)(i):

(A) Health IT must be able to create the following document types regardless of the setting for which it is designed: Diagnostic Imaging Report; Unstructured Document; Enhanced Operative Note Document; Enhanced Procedure Note Document; and Interval Document.

(B) Ambulatory setting only. Health IT must be able to create an Enhanced Encounter Document.

(C) Inpatient setting only. Health IT must be able to create an Enhanced Hospitalization Document.

(ii) Digital signature. (A) Applying a digital signature. Technology must be able to apply a digital signature in accordance with the implementation specification adopted at § 170.205(a)(5)(ii) to a document formatted according to the following standard and applicable implementation specifications adopted at § 170.205(a)(4) and (a)(5)(i). It must also be able to demonstrate that it can support the method for delegation of right assertions.

(1) The cryptographic module used as part of the technology must: be validated to meet or exceed FIPS 140-2 Level 1; include a digital signature system and hashing that are compliant with FIPS 186-2 and FIPS 180-2; and store the private key in a FIPS-140-2 Level 1 validated cryptographic module using a FIPS-approved encryption algorithm. This requirement may be satisfied through documentation only.

(2) Technology must support multi-factor authentication that meets or exceeds Level 3 assurance as defined in NIST Special Publication 800-63-2.

(3) After ten minutes of inactivity, technology must require the certificate holder to re-authenticate to access the private key.

(4) If implemented as a software function, the system must clear the plain text private key from the system memory to prevent the unauthorized access to, or use of, the private key when the signing module is deactivated.

(5) Technology must record time and date consistent with the standard adopted at § 170.210(g).

(B) Validating a digital signature. Technology must be able validate a digital signature that has been applied to a document according to the implementation specification adopted at § 170.205(a)(5)(ii).

(iii) Author of record level 1. Using the same system capabilities expressed in paragraph (i)(1)(ii), technology must be able to apply a digital signature according to the implementation specification adopted at § 170.205(a)(5)(iii) to sign single or bundles of documents a document formatted according to the following standard and applicable implementation specifications adopted at § 170.205(a)(4) and (a)(5)(i).

(iv) Transactions. Using the same system capabilities expressed in paragraph (i)(1)(ii) of this section, technology must be able to apply a digital signature according to the implementation specification adopted at § 170.205(a)(5)(iv) to a transaction and include the signature as accompanying metadata in the signed transaction.

Preamble FR Citation: 80 FR 16864	**Specific questions in preamble?** *No*

Public Comment Field:

The TSSWG directs ONC to the summary of the July 2013 Health IT Standards Committee (HITSC) meeting in which representatives of the Centers for Medicare and Medicaid Services (CMS) presented their objectives and draft plans for the electronic submission of medical records (esMD) specification (available at: http://www.healthit.gov/FACAS/sites/faca/files/2013-07-17_HITSC_summary_final.pdf). At that time, the HITSC expressed serious concerns about advancing a digital signature standard that may conflict with the existing Drug Enforcement Administration (DEA) standard for electronic prescribing of controlled substances, and questioned why the DEA standard had not been leveraged. The HITSC also expressed strong concerns associated with changes to existing administrative and clinical workflows that would be required to integrate esMD into operations.

CMS acknowledged that it would take the HITSC's concerns under advisement and make appropriate changes. As part of its assessment of the readiness of esMD, the TSSWG heard testimony from CMS comparing the digital signature standard incorporated in the esMD specification with the DEA e-prescribing regulation and determined that these standards are now consistent with each other, with the acknowledgement that the esMD standard must allow for sections of a document to be digitally signed, in addition to a digital signature for the document as a whole. CMS also asserted that the esMD specification proposed by the NPRM contains no inherent workflow and that the esMD capability can be provided by a Health IT Module natively or through an external interface. CMS acknowledged that esMD has been implemented only by three small vendors, and they are talking with larger vendors about its consistency with DEA digital signatures.

As for readiness to become a national standard, the TSSWG would note that esMD is a very new specification that is associated with the C-CDA Release 2, which has not yet been widely adopted. Assessed against the HITSC metrics for specification maturity and implementability, **esMD is not ready to be adopted as a standard for certifying HIT**.

In sum, the TSSWG commends CMS for the work they have done to address the concerns expressed by the HITSC. However, **the TSSWG recommends that ONC not adopt esMD as a standard for HIT certification in the 2015 Edition**. The **Workgroup further recommends that ONC work with CMS** to ensure that appropriate efforts are made to **harmonize esMD digital signature standards and requirements with current DEA standards and requirements**, which are already widely adopted, and to encourage piloting, refinement, and adoption of the esMD specification.

C-CDA Data Provenance Request for Comment **pp. 110-111, 167-168 (Public Inspection Version Numbering)**	
Included in 2015 Edition Base EHR Definition? No	
Stage 3 MU Objective N/A	
2015 Edition Health IT Certification Criterion In April 2014, ONC launched the Data Provenance Initiative within the Standards and Interoperability (S&I) Framework to identify the standards necessary to capture and exchange provenance data, including provenance at time of creation, modification, and time of exchange. . . . In the fall of 2014, the HL7 IG for CDA Release 2: Data Provenance, Release 1 (US Realm) (DSTU) was published. This IG clarifies existing content from various standards within HL7 and describes how provenance information for a CDA document in a health IT system should be applied, and what vocabulary should be used for the metadata. . . . We seek comment on the maturity and appropriateness of this IG for the tagging of health information with provenance metadata in connection with the C– CDA. Additionally, we seek comment on the usefulness of this IG in connection with certification criteria, such as ToC and VDT certification criteria.	
Preamble FR Citation: 80 FR 16834 (also see 80 FR 16850)	**Specific questions in preamble?** *Yes*

Public Comment Field:

The TSSWG supports the concept that providers and patients should be able to easily reference and understand the provenance of health information; however, the TSSWG's assessment of the HL7 IG for CDA Release 2: Data Provenance, Release 1 (US Realm) **is that it is not yet ready to be adopted as a national standard for HIT certification**, per the Heath IT Standards Committee's standards readiness model. We understand that the provenance attributes contained in the IG are not new – they were already in the C-CDA specification, but were not well understood – and that the purpose of creating the Provenance IG was to draw out these attributes. We also understand that the IG was updated to incorporate inputs from the HITSC Provenance Task Force prior to publication as part of HL7 DSTU1 (Draft Standard for Trial Use).

We would note that in addition to the Provenance IG, HL7 is also working on a FHIR Provenance-Content specification. While these two efforts are collaborative, it is not clear at this point whether one of these, both of these, or neither of these specifications should ultimately be adopted as the national standard for HIT certification. What is clear is that at this point, neither of these specifications is ready for adoption as a national standard for HIT certification.

The TSSWG urges caution before promoting the Provenance IG specification as a national standard. Because of its very limited adoption, it is difficult to judge how easily it can be implemented and integrated into operational workflows. Given the significant role that data provenance plays in data quality and data integrity, the TSSWG encourages **ONC to support continued development, piloting, use, and refinement of the HL7 Provenance IG and FHIR Provenance-Content specification**.