



Privacy and Security Tiger Team

**Comparison of Stage 2 Proposed Rules
w/Health IT Policy Committee previous
privacy & security recommendations**

Preliminary Recommendations

April 4, 2012

Tiger Team Members

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, SAIC
- **Dan Callahan**, Social Security Administration
- **Neil Calman**, Institute for Family Health
- **Carol Diamond**, Markle Foundation
- **Judy Faulkner**, EPIC Systems Corp.
- **Leslie Francis**, University of Utah; NCVHS
- **Gayle Harrell**, Consumer Representative/Florida
- **John Houston**, University of Pittsburgh Medical Center
- **Alice Leiter**, National Partnership for Women & Families
- **David McCallie**, Cerner Corp.
- **Wes Rishel**, Gartner
- **Latanya Sweeney**, Carnegie Mellon University
- **Micky Tripathi**, Massachusetts eHealth Collaborative

HHS Staff assistance:

- **Joy Pritts**, ONC
- **Verne Rinker**, OCR

Goal of Today's Discussion

- Report on New ONC Guidance to State HIE Grantees (builds from previous Health IT Policy Committee privacy and security policy recommendations)
- Review treatment of Committee's privacy and security recommendations in Proposed Stage 2 rules
- Begin discussing recommendations for Stage 2

Announcement – New ONC Guidance to State HIE Grantees

- http://healthit.hhs.gov/portal/server.pt/gateway/PTARG_S_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf
- Provides guidance to state grantees and requires them to submit privacy and security frameworks
- The guidance “builds from the privacy and security and governance recommendations of the Health IT Policy Committee...”
- Includes adoption of policies based on ONC’s articulation of fair information practices and consent

Previous Recommendations Aimed at Stage 2 of Meaningful Use and Certification

- Security risk assessment & addressing encryption of data at rest
- Capability to support amendments
- Patient portals (view/download/transmit function)
- Patient matching – standard formats for demographic data fields, address normalization
- E-prescribing of controlled substances
- Digital certificates for exchange
- Certification of EHR modules for privacy & security

Status of Recommendations

- Fully adopted:
 - Security Risk Assessment, including addressing encryption of data at rest
 - Amendments – provisions regarding capability to make amendments and append additional information
 - Patient Portals – requirement for patient accessible audit log of portal access
- Not Sure (no express adoption but may be covered by other standards such as CCDA & transport):
 - Patient Portals: data provenance
 - Patient Matching: standard formats for fields used for matching, missing data
 - Digital Certificates: use of digital certificates (or some form of entity authentication with high degree of assurance)

Status of Recommendations

- Not adopted
 - Amendments: capability to transmit amendments to other providers by Stage 3
 - Patient Portals: secure download, authentication, mechanism to block programmatic or unauthorized attacks
 - EHR modules
 - E-prescribing of Controlled Substances (EHR capability)
 - Digital certificates: testing of use
 - Patient Matching and Demographics: address normalization, testing of demographic formats

Tiger Team Suggestions for Policy Committee Comments on Proposed Rules (1)

- Comment favorably on CMS' proposal to include the security risk assessment (currently in Stage 1) and attesting to addressing encryption of data at rest in Stage 2 as privacy and security MU criteria
- With respect to amendments, comment favorably on ONC's proposal to require that Certified EHR Technology have the capability to make amendments to a patient's health data and be able to append information from the patient & any rebuttal from the entity regarding the data (per HIPAA requirements).
 - EHR Technology should be required to append patient-supplied information in both free text and scanned formats (specific question from ONC).

Tiger Team Suggestions for Policy Committee

Comments on Proposed Rules (2)

- Request that ONC signal in the final Stage 2 rule that by Stage 3 of MU, Certified EHR Technology must demonstrate the capability to transmit amendments (plus appended information) to other providers
- Comment favorably on ONC's proposal to require patient accessible log in Stage 2 certification

Issues Requiring Further Tiger Team Discussion (1)

(Discussing jointly with Standards Committee partners)

- Portals (view/download/transmit)
 - Require testing of certified EHR technology for authentication of patients (using at least single factor) and secure download
 - Proposed rule states that such technical implementations are commonplace & ubiquitous and therefore do not need to be required for certification
 - Require certified EHR technology to include requirements for data provenance that is accessible to patient/user (CCDA?)
 - Require certified EHR technology to include capability to detect and block programmatic and unauthorized user attacks (note: Standards Committee put forth different recommendation)
 - Urge ONC to more formally endorse guidance recommendations and develop and implement dissemination strategy

Issues Requiring Further Tiger Team Discussion (2) (Discussing jointly with Standards Committee partners)

- EHR Modules
 - Stage 1 final certification requirements required EHR modules to be tested for all privacy and security certification requirements (except in certain circumstances)
 - Stage 2 proposed rule eliminates this requirement and instead requires the Base EHR to be certified for all privacy and security requirements.
 - Standards Committee adopted a different recommendation
 - Currently assessing whether proposed approach is sufficient or leaves gaps

Issues Requiring Further Tiger Team Discussion (3) (Discussing jointly with Standards Committee partners)

- E-Prescribing of Controlled Substances
 - DEA rules require providers to comply with 2-factor authentication requirements when prescribing controlled substances
 - Policy Committee recommended that certified EHR Technology have capability to support such authentication
 - ONC declined to propose for Stage 2, noting potential policy conflicts with state law and challenges with widespread ability of products that include functionalities to support DEA requirements
 - ONC requests comment on availability point.
 - Tiger Team considering whether to push for capability in Stage 2 or strong signal from ONC for Stage 3

Issues Requiring Further Tiger Team Discussion (4) (Discussing jointly with Standards Committee partners)

- Digital Certificates
 - Policy Committee recommended entity-level digital certificates issued with high degree of assurance
 - Committee also recommended that certified EHR technology be tested on use of such certificates for appropriate transactions
 - Not addressed in proposed Stage 2 rule
 - Requirements for exchange for meaningful use are proposed to be increased in Stage 2. Tiger Team exploring whether additional recommendations for Stage 2 certification are needed to ensure entity-to-entity authentication (for example, are entity authentication issues addressed in proposed transport standards?).

Issues Requiring Further Tiger Team Discussion (5) (Discussing jointly with Standards Committee partners)

- Patient Matching
 - Consider whether demographic data fields in CCDA (including null flavors for missing data) satisfy Policy Committee's recommendations regarding standardization of demographic data fields.
 - In particular, consider reinforcing previous recommendation that certification criteria include testing that appropriate transactions are sent and received with correct data formats and data entry sequences exist to reject incorrectly entered values.
 - Also consider whether to further push for USPS normalization of addresses.
 - Consider ONC's request for comment on whether EHR technology should be able to perform matching between the patient in the EHR technology and the summary of care document about to be incorporated.

Backup Slides

Amendments

Speaker's Note: Legal requirements for amendments included in Backup Slide #

HITPC Recommendation:

- Certified EHR technology should have the capability to support amendments, including a provider's compliance with HIPAA requirements to respond to patient requests for amendments:
 - Make amendments to the patients health information in a matter consistent with the entity's obligations with regard to the legal medical record (i.e., ability to view the original data and identify changes).
 - Append information from the patient and any rebuttal from the entity regarding the data.

Amendments (continued)

Proposed Rule(s):

- Certification NPRM states that certified Complete EHRs and EHR modules must have the capability to:
 - Enable a user to electronically amend a patient’s health record to:
 - Replace existing information in a way that preserves the original information; and
 - Append patient supplied information, in free text or scanned, directly to a patient’s health record or by embedding an electronic link to the location of the content of the amendment.
 - Enable a user to electronically append a response to patient supplied information in a patient’s health record.

Amendments (continued)

- Also **specifically requests comment** on whether EHR technology should be required to be capable of appending patient supplied information in both free text and scanned format or only one of these methods to be certified to this proposed certification criteria.

Comment Options:

- Tentative decisions reached at previous meeting:
 - Comment praising ONC for adopting recommendation on patient amendments; and
 - Comment that the technology should be required to append patient-supplied information in both free text and scanned formats.

Amendments (continued)

HITPC Recommendation (Not Adopted):

- Certified EHR technology should have the ability by MU Stage 3 to transmit amendments, updates, or appended information to other providers to whom the data in question has been previously transmitted.
 - Recommendation was narrow in scope and intended only to enable providers to transmit amendments, updates, or appended information to other providers as required by law or as desired by providers.
 - It was not intended, for example, to require that the technology have the capability to identify recipients with whom the information was shared.

Amendments (continued)

Proposed Rule(s):

- Not addressed in either rule.
- Outstanding question for TT discussion: Does the adoption of transport standards address this capability?

Comment Options:

- No comment.
- Comment that:
 - It is important that certified technology enable providers to propagate amendments, updates, and appended information to other providers, consistent with existing requirements.
 - The preamble for final rule should include language clearly signaling ONC's intention to require this capability in Stage 3.

Patient Portals (View/Download/Transmit)

HITPC Recommendations:

- Patient portals should include mechanisms that ensure information in the portal can be securely downloaded to a third party authorized by the patients.
- Providers should require at least a user name and password to authenticate patients. This single factor authentication should be a minimum.

Patient Portals (continued)

Proposed Rules:

- MU Rule
 - More that 10 percent of all unique patients seen by the EP, EH, or CAH, view, download or transmit to a third party their health information.
- Certification Rule
 - Certified EHRs must have the ability to transmit a summary care record to a third party
 - ONC did not include capabilities for single factor authentication and secure download, stating that such technical implementations are commonplace and ubiquitous and thus, little value would derive by requiring these capabilities as a condition of certification.

Patient Portals (continued)

Comment Options:

- No comment
- Comment
 - While technical implementations of secure download and single-factor authentication may be widespread, these capabilities should be required as a condition of certification to ensure that they are included in all EHR technology and continue to be available into the future.
 - One of our goals in recommending these capabilities be included as certification criteria was to have them tested.
 - Reiterate recommendations to include these capabilities as a condition for certification in Stage 2.

Patient Portals (continued)

Speaker's Note: The Consolidated CDA prescribes standard formats, for example, for Author (created content), Data Enterer (transferred content to clinical document), Informant (source of content), Legal Authenticator (single person legally responsible for the document), etc. (HL7 Implementation Guide for CDA).

HITPC Recommendation (Not Sure):

- Patient portals should include appropriate provisions for data provenance, which is accessible to the user, both with respect to access and upon download.

Proposed Rules:

- Certification rule asserts that the adoption of the Consolidated CDA standard addresses the recommendation to include “data provenance” with any health information that is downloaded.
- CDA prescribes standard formats for Author, Data Enterer, Legal Authenticator, etc.

Patient Portals (continued)

Comment Options:

- No comment; defer to Standards Committee.
- Praise ONC for adopting the Consolidated CDA standard, as it addresses the need for data provenance with downloaded health information.
- Praise ONC for adopting the Consolidated CDA standard but raise any specific areas in which the standard does not go far enough in addressing data provenance.

Patient Portals (continued)

HITPC Recommendation (Not adopted):

- Certified EHRs should include a capability to detect and block programmatic attacks or attacks from known but unauthorized persons (such as auto lock-out after a certain number of unsuccessful log-in attempts).

Patient Portals

Proposed Rule(s)

- Not addressed in either rule.
- Note: The HITSC's Privacy and Security Workgroup considered the HITPC's recommendation on blocking programmatic attacks
 - Concluded that this objective/measure does not align well with today's security technology, such as technology that allows entities to federate user identity, (e.g., OpenID, OAuth, SAML)
 - Recommended that the HITSC ask the HITPC to reconsider this objective/measure as a potential "guidance" or "good practice" statement rather than as policy to be implemented in EHR technology.

Patient Portals

Comment Options

- No comment
- Comment by
 - Referencing Standards Committee views on this recommendation and
 - Recommending that ONC cite this capability as a best practice in the preamble to the final rule.
- Comment by
 - Referencing Standards Committee views on this recommendation and
 - Reiterating recommendations that this be included in certification criteria. (Need rationale)

Patient Portals

HITPC Recommendation (Not Sure):

- Best practices—as opposed to certification criteria—for providers, vendors, and software developments for providing guidance to patients using the view/download functionality.

Proposed Rule(s):

- MU NPRM notes this recommendation and states hospitals can sponsor education and awareness activities that result in patients viewing their information.

Patient Portals (continued)

Comment Options:

- No comment.
- Comment by
 - Reiterating the importance of patient education on the use of the view/download capability to encourage protection of the information and
 - Recommending that ONC reference recommendation on guidance in the preamble to the final rule and commit to provide such guidance through, for example, its Regional Extension Center (REC) program.

EHR Modules

Speaker's Note: See HITPC Recommendations at link; April 2010 meeting.

HITPC Recommendation (Not Adopted):

- In commenting on Stage 1 MU NPRM, the [Privacy and Security Workgroup](#) (precursor to the P&S Tiger Team) strongly endorsed a default rule that all EHR modules must meet all privacy and security certification criteria.

EHR Modules (continued)

Related HITSC Recommendation

- To enable the certification process to more effectively address security integration, the P&S Workgroup recommends that the ONC and NIST consider modifying the certification process so that each privacy and security certification criterion is treated as “addressable.” To meet the criterion, each Complete EHR or EHR Module submitted for certification would need to either:
 - Implement the required security functionality within the complete EHR or EHR module(s) submitted for certification; or
 - Assign the function to a 3rd party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion.

EHR Modules (continued)

Proposed Rules:

- Certification NPRM:
 - Proposes not to apply the privacy and security certification requirements for the certification of EHR Modules, citing stakeholder feedback, particularly from EHR technology developers, that identified that this regulatory requirement is causing unnecessary burden (both in effort and cost).
 - ONC stated: Based on our proposal that EPs, EHs, and CAHs must have a Base EHR to meet our proposed revised definition of CEHRT that would apply beginning with FY/CY 2014, we believe that we can be responsive to stakeholder feedback with our proposal not to apply the privacy and security certification requirements to EHR modules, while still requiring an equivalent or higher level of privacy and security capabilities to be part of CEHRT.

EHR Modules (continued)

Comment Options:

- No comment; defer to Standards Committee to address.
- Comment by endorsing Standards Committee recommendation as a way of addressing compliance burden, while providing appropriate privacy and security protections.
- Comment by
 - Underscoring the risks associated with not requiring compliance with privacy and security criteria and
 - Reiterating recommendation that EHR modules must meet all privacy and security certification criteria.

E-prescribing Controlled Substances

HITPC Recommendation (Not Adopted):

- EPs are required to comply with the DEA rule regarding e-prescribing of controlled substances. Certification testing criteria should include testing of compliance with the DEA authentication rule, which requires 2-factor authentication.

E-prescribing Controlled Substances (continued)

Proposed Rule(s):

- MU NPRM:
 - Some challenges remain including more restrictive State law and widespread availability of products that include the functionalities required by the DEA's regulations.
 - **Encourages comments** addressing the current and expected availability of these products and whether the availability would be sufficient to include controlled substances.

E-prescribing Controlled Substances (continued)

Comment Options:

- No comment; or
- Comment that sufficiently developed technology should be available by the time that MU rules go into effect; ONC should require this capability as part of Stage 2 certification requirements; or
- Comment that the needed technology may not be available by the time that MU rules go into effect; ONC should, however, strongly signal in the preamble that this capability will be a requirement for Stage 3.

Digital Certificates

HITPC Recommendation (Not Sure):

- EPs and EHs should be required to obtain digital certificates per previous P&S TT recommendations.
- EHR certification process should include testing on the use of digital certificates for appropriate transactions.

Digital Certificates (continued)

Speaker's Note: I have been unable to get an answer to the question of whether the transport standards require use of digital certificates.

Proposed Rule(s):

- Not addressed in either rule.
- Outstanding question for TT discussion: Do required transport standards require use of digital certificates?

Comment Options:

- No comment; or
- Comment by highlighting the importance of digital certificates for authentication and reiterating recommendation.

Patient Matching and Demographics

Speaker's Note: Any SHALL conformance statement may use nullFlavor, unless the attribute is required.

HITPC Recommendations:

- HITSC should:
 - Identify standard formats for data fields that are commonly used for matching patients (for ex: name, DOB, zip, address, gender)(Not Sure),
 - Specify standards that describe how missing demographic data should be represented during exchange (Not Sure), and
 - Consider whether USPS normalization would be beneficial to improved matching accuracy and whether it should be added to the demographic standards (Not Adopted).
- Certification criteria should include testing that (1) appropriate transactions are sent/received with correct demographic data formats and (2) data entry sequences exist to reject incorrectly entered values (Not Adopted).

Patient Matching and Demographics (continued)

Speaker's Note: I am still obtaining additional information on how to interpret the standard's use of nullFlavors.

Proposed Rules:

- Certification NPRM:
 - Adopted the Consolidated CDA as a requirement, which includes:
 - standards for name, gender, address, date of birth, telephone number, and zip code contained in the document header and
 - “null flavors” to designate missing information, which may be used to address required fields.
 - Did not address normalization and testing.
 - **Requested public comment** on whether ONC should require, as part of the “incorporate summary care record” certification criterion, that EHR technology be able to perform some type of demographic matching or verification between the patient in the EHR technology and the summary care record about to be incorporated. This would help prevent two different patients' summary care records from being combined.

Patient Matching and Demographics (continued)

Comment Options:

- Standards for data fields used for matching
 - No comment/defer to Standards Committee, or
 - Praise ONC for adopting the Consolidated CDA, which should facilitate patient matching, or
 - Praise ONC for adopting the Consolidated CDA, but comment on any standards needing revision.
- Normalization
 - No comment, or
 - Re-emphasize the importance of address normalization and recommend that ONC include address normalization as part of certification.

Patient Matching and Demographics (continued)

- Testing
 - No comment, or
 - Re-emphasize the importance of testing as part of the certification process and recommend that the final rule include testing as recommended by the HITPC.
- Comments on demographic matching by EHR technology
 - No comment, or
 - Agree that, as part of the “incorporate summary care record” certification criterion, that EHR technology be able to perform demographic matching between the patient in the EHR technology and the summary care, or
 - Disagree that demographic matching should be included in the “incorporate summary care record” certification criterion.