# Health IT Standards Committee

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

October 21, 2011

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Mostashari:

This transmittal memo presents additional complementary recommendations related to the certification criteria, standards, and implementation specifications for EHR technology certification we previously transmitted to you on September 28, 2011.

Upon the Implementation Workgroup's presentation to the HIT Standards Committee, the Privacy and Security Workgroup completed a subsequent analysis focused on those certification criteria that were related to privacy and security. The Privacy and Security Workgroup presented its analysis to the HIT Standards Committee on October 21, 2011 and they were accepted for transmittal to ONC. We recommend that ONC refer to the attached matrix of draft standards, implementation specifications and certification criteria to inform its notice of proposed rulemaking. We believe these recommendations will serve as an effective starting point for the rulemaking that will take place to support the next stage of meaningful use.

Sincerely yours,

| /s/ | /s/ |
|---|---|
| Jonathan Perlin | John Halamka |
| Chair, Health IT Standards Committee | Vice Chair, Health IT Standards Committee |

Attachment: P&S Certification Criteria Matrix

# HITSC Privacy and Security Workgroup recommendations for Stage 2 Meaningful Use Certification Criteria, Standards, and Implementation Specifications

**GENERAL RECOMMENDATION**

While discussing potential privacy and security criteria for Stage 2, we often found ourselves discussing whether "the EHR" (Complete or Module) submitted for certification should be expected to meet a given criterion, or whether the EHR could depend upon some other system component (e.g., operating system) or external service to meet the criterion. Given that many privacy and security functions and assurances are provided by the infrastructure in which an "EHR" operates, one might reasonably assume that the EHR itself would not need to provide basic, foundational security functions and assurances. Indeed, we believe that EHR technology should depend primarily upon infrastructure assurances and specialized security services, and that the EHR itself should provide only those security services that are specific to protecting the confidentiality, integrity, and availability of electronic health information. The Workgroup ultimately agreed that throughout our recommendations, we would use the term "EHR" to include the Complete EHR or EHR Module(s) submitted for certification, plus any infrastructure and third-party services that the EHR technology may rely upon to meet the criterion.

We see the integration of EHR, infrastructure, and specialized security products and services as key to protecting electronic health information, care quality, and patient safety. To enable the certification process to more effectively address security integration, we recommend that the ONC and NIST consider modifying the certification process so that each privacy and security certification criterion is treated as "addressable," similar to how the implementation specifications in the HIPAA Security Rule are "addressable." That is, to meet each security criterion, each Complete EHR or EHR Module submitted for certification would need to either:

1) Implement the required security functionality within the Complete EHR or EHR Module(s) submitted for certification; or

2) Assign the function to a third-party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion.

We would welcome further discussion of this concept.

**OTHER GENERAL COMMENTS**

1. For the regulation, we recommend grouping all of the objectives/measures addressing patient-communications together – i.e., Rows 22-26 and 46-50. We also suggest moving the patient authentication objective/measure to precede the patient secure messaging requirement – as we have done here.

2. In the Objectives/Measures relating to consumer communications, we recommend replacing the terms “patient online account” and “patient portal” with “consumer web-based application” to avoid implying a specific architecture.

3. The objective/measure dealing with amendments to health records (IWG Ref 52) extends beyond the scope of privacy and security. We recommend the Implementation Workgroup have an expert in medical records review the criteria we have suggested here.

# RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| 46 | Privacy and Security<br><br>**(NEW)** Single Factor Authentication (~~Patient Online Account~~) .<br><br>Consumer Web-Based Application | | EHR must be able to authenticate the identity of an authorized patient or their personal representative using single-factor authentication (or stronger) based on the standard specified. | STANDARD:<br>NIST SP 800-63, Level 2 (single-factor authentication) |
| 26 | Secure Messaging<br><br>EPs: **(NEW)** Patients are offered secure messaging online and at least 25 patients have sent secure messages online | | EHR must provide the capability to send messages to, and receive messages from, patients using a mechanism that assures that (1) the identity of the patient is authenticated; (2) the identity of the EHR is authenticated; and (3) message content is encrypted and integrity protected. | EXAMPLE STANDARDS:<br>FIPS Pub 140-2, Annex A;<br>IETF RFC 2246 (TLS 1.0);<br>SMTP/SMIME<br><br>IMPLEMENTATION SPEC:<br>NIST SP 800-52 (TLS);<br>NwHIN Transport Specifications . |
| 47 | **(NEW)** Audit Trails for Access to ~~Patient Online Account~~ .<br>Consumer Web-Based Application | | [**COMMENT:** Covered by general audit criteria] . | |
| 48 | Privacy and Security<br><br>**(NEW)** Establish Data Provenance for ~~Patient Portal~~ .<br><br>Consumer Web-Based Application | | EHR must be able to create and include data-provenance information with any health data downloaded by the patient (e.g., lab that reported test results) or sent to a patient's PHR. | |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| 49 | Privacy and Security<br><br>**(NEW)** Patient Portal - Secure Download Ability | | EHR must enable the patient to download a copy of his or her health information over a secured communication channel. | |
| 50 | Privacy and Security<br><br>**(NEW)** Warning Message Before Downloading PHI. from Consumer Web-Based Application | | [**COMMENT**: The P&S Workgroup agrees with the Implementation Workgroup's assessment of this objective/measure as outside the scope of certification. Further, in considering the potential implications of this policy for EHR technology, we recommend 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.] | |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| **34** | Perform, or update, security risk assessment and address deficiencies.<br><br>Address encryption for data at rest. EPs and EHs attest to this policy. | § 170.302(o)<br><br>Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information. | [No change is recommended for Stage 2.] | IMPLEMENTATION SPEC:<br>ASTM, E1986-09 (Information Access Privileges To Health Information) |
| **35** | | § 170.302(p)<br><br>Emergency access. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency. | [No change is recommended for Stage 2.] | |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| 36 | (continued)<br>Perform, or update, security risk assessment and address deficiencies.<br><br>Address encryption for data at rest. EPs and EHs attest to this policy. | § 170.302(q)<br><br>Automatic log-off. Terminate an electronic session after a predetermined time of inactivity. | (1) EHR must be able to initiate a session lock after a designated period of inactivity or upon receiving a request from a user.<br>(2) Once a session has been locked, EHR must retain the session lock until the user reestablishes access using an authorized identifier and authenticator.<br>(3) EHR must be able to terminate an electronic session (i.e., automatically log a user off) after an established period of inactivity.<br>(4) EHR must provide the capability for a system administrator to set time periods for electronic session locking and termination. | IMPLEMENTATION SPEC:<br>NIST SP 800-53, Rev 3 |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| 37 | (continued)<br>Perform, or update, security risk assessment and address deficiencies.<br><br>Address encryption for data at rest. EPs and EHs attest to this policy. | § 170.302(r)<br><br>Audit log.<br>(1) Record actions. Record actions related to electronic health information in accordance with the standard specified in § 170.210(b).<br>(2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at § 170.210(b). | Activity auditing.<br>(1) Detect and record auditable events. (a) EHR must be able to detect auditable events. (b) EHR must be able to record information about security-relevant events, in accordance with the standard specified in §170.210(b).<br>(2) Protect audit information. (a) EHR must assure that audit data cannot be modified, overwritten, or deleted. (b) EHR must be able to detect attempts to alter audit data.<br><br>Generate audit report(s). EHR must enable a user to generate an audit report for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at 170.210(b). | STANDARD: Record audit data about security-relevant events.<br><br>IMPLEMENTATION SPEC:<br>ASTM E2147-01, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems; |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| **38** | (continued)<br>Perform, or update, security risk assessment and address deficiencies.<br><br>Address encryption for data at rest. EPs and EHs attest to this policy. | § 170.302(s)<br><br>Integrity.<br>(1) Create a message digest in accordance with the standard specified in 170.210(c).<br>(2) 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.<br>(3) Detection. Detect the alteration of audit logs. | Integrity.<br>(1) Create a message digest in accordance with the standard specified in 170.210(c).<br>(2) 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. | STANDARD:<br>Change to "SHA-1 or SHA-1 plus SHA-2" |
| **39** | | § 170.302(t)<br><br>Authentication. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. | (1) Person Authentication. EHR must be able to authenticate human users who assert an identity and present at least one proof of that identity.<br><br>(2) Entity Authentication. EHR technology must authenticate the identity of external entities before sending any electronic health information to them, or receiving any electronic health information from them. | STANDARD:<br>NIST SP 800-63, Level 2 (single-factor authentication);<br>ITU-T X.509 |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| **40** | (continued)<br>Perform, or update, security risk assessment and address deficiencies.<br><br>Address encryption for data at rest. EPs and EHs attest to this policy. | § 170.302(u)<br><br>General encryption. Encrypt and decrypt electronic health information in accordance with the standard specified in §170.210(a)(1), unless the Secretary determines that the use of such algorithm would pose a significant security risk for Certified EHR Technology. | General encryption. EHR must be able to encrypt and decrypt electronic health information in accordance with the standard specified in §170.210(a)(1).<br><br>(1) Data-at-rest encryption. EHR technology whose functionality includes the capability to manage electronic PHI on end-user device storage must be able to encrypt and decrypt data persisted on those end-user devices. | STANDARD:<br>FIPS Pub 140-2, Annex A<br>[No change from Stage 1; FIPS Pub 140-3 is still in draft so we believe it would be premature to specify as the standard]<br><br>IMPLEMENTATION SPEC:<br>NIST SP 800-111 |
| **41** | | § 170.302(v)<br><br>Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2). | (2) Encryption when exchanging electronic health information. EHR technology must assure that all health information exchanged with external entities is encrypted and integrity-protected. | STANDARDS:<br>FIPS Pub 140-2, Annex A;<br>IETF RFC 2246 (TLS 1.0);<br>IETF RFC 2401 (IPsec)<br><br>IMPLEMENTATION SPEC:<br>NIST SP 800-52 (TLS);<br>NIST SP 800-77 (IPsec VPN); NIST SP 800-113 (SSL VPN);<br>other transport or network layer protocols validated i.a.w. FIPS Pub 140-2<br><br>NwHIN transport standards |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| 42 | (continued)<br>Perform, or update, security risk assessment and address deficiencies.<br><br>Address encryption for data at rest. EPs and EHs attest to this policy. | § 170.302(w) ***Optional***<br><br>Accounting of disclosures. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d). | [No change is recommended for Stage 2.] | |
| 43 | Privacy and Security<br><br>**(NEW)** Address encryption for data at rest for data located in datacenters and in mobile devices (e.g. laptops, PDAs, etc.)). EPs and EHs attest to this policy. | | [P&S WG agrees with Implementation WG – out of scope] | |
| 44 | Privacy and Security<br><br>**(NEW)** 2-Factor Authentication For Controlled Substances (Providers) | | [P&S WG agrees with Implementation WG – out of scope] | |
| 45 | Privacy and Security<br><br>**(NEW)** Entity Level Digital Certificates (Providers) | | [P&S WG agrees with Implementation WG – out of scope] | |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| 51 | Privacy and Security<br><br>**(NEW)** Capability to detect and block programmatic attacks or attacks from a known but unauthorized user (such as auto lock-out after a certain number of unsuccessful log-in attempts) | | [**COMMENT**: In considering the potential implications of this policy for EHR technology, the P&S Workgroup 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). We recommend 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.] | |

## RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

| IWG Ref | HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC | Stage 1 Adopted Certification Criterion Ambulatory /Inpatient | HITSC Privacy and Security Workgroup Recommendations | |
|---|---|---|---|---|
| | | | Recommended New or Revised Certification Criterion | Recommended Standard(s) and/or Implementation Specification(s) |
| 52 | Amendments<br><br>**(NEW)** CEHRT should make it technically possible for providers to:<br>(1) Make amendments to a patient's health information in a way that is consistent with the entity's obligations with respect to the legal medical record (i.e., there should be the ability to access/view the original data and to identify any changes to it)<br>(2) Append information from the patient and any rebuttal from the entity regarding disputed data | | (1) EHR must provide the capability for an authorized provider to amend health information, while preserving the integrity of the data originally recorded in the health record.<br>(2) EHR must provide the capability to attach to health information: (a) patient-asserted information, or an electronic link to patient-asserted information; and (b) a provider's formal rebuttal to patient-asserted information.<br>(3) EHR must maintain an audit trail of the amendments to health information (1 and 2 above). | |

# RECOMMENDATIONS REGARDING CONSUMER COMMUNICATIONS

**KEY**

This table is designed for printing on legal paper (8.5" x 14").

Column 1 = Row number assigned by the Implementation Workgroup
Column 2 = HITPC proposals for MU Stage 2, including new objectives and measures and the elimination or "combining of objectives (and measures)." In addition, column includes HITPC recommendations to HITSC.
Column 3 = Current certification criteria
Column 4 = Privacy and Security Workgroup's recommended new or revised certification criterion.
Column 5 = Privacy and Security Workgroup's recommended standard(s) and/or implementation specification(s) to support MU Stage 2.

***Font Colors***

Black = Objectives/measures/certification criteria/standards/implementation specifications related to both ambulatory and inpatient settings.
Blue = Objectives/measures/certification criteria related only to the ambulatory setting.
Red = Objectives/measures/certification criteria related only to the inpatient setting.
Turquoise = HITSC Privacy and Security Workgroup recommendations