

# **HIT Standards Committee**

## **Privacy and Security Workgroup**

### **Stage 2 Meaningful Use Privacy and Security Recommendations**

**Dixie Baker, Chair**  
**Walter Suarez, Co-Chair**

**October 21, 2011**

# Privacy and Security Workgroup

- Dixie Baker, SAIC
- Anne Castro, BlueCross BlueShield of South Carolina
- Aneesh Chopra, Federal Chief Technology Officer
- Mike Davis, Veterans Health Administration
- Lisa Gallagher, HIMSS
- Chad Hirsch, Mayo
- Ed Larsen
- David McCallie, Cerner Corporation
- John Moehrke, General Electric
- Steve Findlay, Consumers Union
- Jeff Jonas, IBM
- Wes Rishel, Gartner
- Walter Suarez, Kaiser Permanente
- Sharon Terry, Genetic Alliance

## Process

- HITSC received from the HIT Policy Committee (HITPC) draft Stage 2 Meaningful-Use objectives/measures and other directions
- HITSC Implementation Workgroup requested inputs from the Privacy and Security Workgroup on security- and privacy-related objectives/measures and directions, including patient/consumer communications
  - In some cases, Implementation Workgroup offered suggestions
- Privacy and Security Workgroup reviewed all measures and suggestions, and recommended certification criteria, standards, and implementation specifications
- Presenting our recommendations to the Implementation Workgroup and the HITSC, today
  - Complete recommendations are included as an Appendix to this document

## General Challenge

- Effective measures and assurances for protecting electronic health information are built into the infrastructure
  - Enterprise network and system architecture
  - Operating systems
  - Database management systems
  - Third-party specialized security services – such as enterprise identity management, audit monitoring and intrusion/misuse detection, virus detection, and public-key infrastructure
- EHR technology should depend primarily upon these infrastructure assurances and specialized security services – the EHR itself should provide only those security services that are specific to protecting the confidentiality, integrity, and availability of the electronic health information it manages

# General Recommendation

- Effective integration of EHR, infrastructure, and specialized security products and services is key to protecting electronic health information, care quality, and patient safety
- Today every Complete EHR and EHR Module must meet all security certification criteria – which tends to encourage the implementation of security services within the EHR, rather than having the EHR use stronger mechanisms provided by the infrastructure or third-party services
- 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” – 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 third-party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion

# Consumer Communications Recommendations

All **NEW** in Stage 2

- Use at least one factor (e.g., password) to authenticate the identity of consumer or personal representative
- Exchange messages securely
  - Authenticate consumer
  - Authenticate EHR
  - Encrypt and integrity protect message
  - Standards: FIPS Pub 140-2, transport layer security (TLS), secure email (SMTP/SMIME)
  - Implementation Specifications: NIST SP 800-52 (TLS); NwHIN transport specifications
- Security download of health information
  - Include data provenance with downloaded information and information sent to PHR
- Warning before PHI download should be “guidance” or “best practice” and not certification criterion

## General Privacy and Security: No Changes

- No changes recommended for the following certification criteria:
  - Access Control
  - Accounting of Disclosures
  - General Encryption
  - Accounting of Disclosures

# General Privacy and Security: Recommended Changes

- Automatic Log-off: Clarify “terminate a session” criterion to include:
  - Session lock after designated period of inactivity
  - Session unlocking with user authentication
  - Session termination (automatic log-off) after designated period of inactivity
  - Capability to designate time periods for session locking and termination
- Audit Log:
  - Change title to “Activity Auditing” (as recommended by IWG)
  - Broaden scope, and allow more selectivity, for security auditing
    - Require detection of, and recording of information about “security-relevant events” – rather than “actions related to electronic health information” only
    - Change standard to “Record audit data about security-relevant events” – replacing limited enumerated list of data elements and events
    - Add ASTM E2147-01 as implementation specification (suggests data elements and events)
  - Add audit-data protection provisions

# General Privacy and Security: Recommended Changes

- Integrity: Add SHA-2 as a standard (but retain SHA-1)
- Authentication: Separate criteria for person vs. entity
  - Person authentication – at least single factor (e.g., password)
  - Entity authentication – X.509 digital certificates
- Encryption: Incorporate provisions of “Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,” issued by the Secretary per ARRA/HITECH breach-notification provisions
  - Add criterion for encryption for data-at-rest on end-user devices:  
“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.”
  - Encryption when exchanging electronic health information:
    - Add standards: transport layer security (TLS), Internet Protocol security (IPsec)
    - Add implementation specifications cited in breach guidance, plus NwHIN transport standards

# General Privacy and Security: **NEW** Objectives/Measures

- Encryption of data at rest in data centers and mobile devices
  - Recommended encryption for data on end-user devices controlled by EHR
  - Encryption of data in data centers is risk-management decision – and out of scope for certification criteria (as suggested by IWG)
- Two-factor authentication: agree with IWG assessment as out of scope
- Entity-level digital certificates: Incorporated into entity authentication criterion
- Detect and block programmatic attacks (e.g., lock-out after allowed number of log-in attempts): does not align well with today's identity authentication technologies; suggested that HITPC consider “guidance” or “best practice” rather than policy
- Amendments to health records:
  - Amendment by authorized provider, while preserving data integrity
  - Attachment of patient assertion and provider rebuttal
  - Audit trail of amendments
  - Recommend the Implementation Workgroup have an expert in medical records review the criteria we have suggested

Appendix: Privacy and Security Workgroup Stage 2  
Meaningful Use Privacy and Security Recommendations  
to Implementation Workgroup

## 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.

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <b>Ambulatory /Inpatient</b>	HITSC Privacy and Security Workgroup Recommendations	
			Recommended New or Revised Certification Criterion	Recommended Standard(s) and/or Implementation Specification(s)
46	Privacy and Security  <b>(NEW)</b> Single Factor Authentication ( <del>Patient Online Account</del> ).  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: NIST SP 800-63, Level 2 (single-factor authentication)
26	Secure Messaging  <u>EPs:</u> <b>(NEW)</b> 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: FIPS Pub 140-2, Annex A; IETF RFC 2246 (TLS 1.0); SMTP/SMIME  IMPLEMENTATION SPEC: NIST SP 800-52 (TLS); NwHIN Transport Specifications.
47	<b>(NEW)</b> Audit Trails for Access to <del>Patient Online Account</del> .  Consumer Web-Based Application		<u>COMMENT:</u> Covered by general audit criteria].	
48	Privacy and Security  <b>(NEW)</b> Establish Data Provenance for <del>Patient Portal</del> .  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.	

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <b>Ambulatory /Inpatient</b>	HITSC Privacy and Security Workgroup Recommendations	
			Recommended New or Revised Certification Criterion	Recommended Standard(s) and/or Implementation Specification(s)
49	Privacy and Security <b>(NEW)</b> 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 <b>(NEW)</b> Warning Message Before Downloading PHI. from Consumer Web-Based Application		<b>[COMMENT:</b> 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.]	

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <b>Ambulatory /Inpatient</b>	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.  Address encryption for data at rest. EPs and EHs attest to this policy.	<p>§ 170.302(o)</p> <p><u>Access control.</u> 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.</p>	[No change is recommended for Stage 2.]	IMPLEMENTATION SPEC: ASTM, E1986-09 (Information Access Privileges To Health Information)
35		<p>§ 170.302(p)</p> <p><u>Emergency access.</u> Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.</p>	[No change is recommended for Stage 2.]	

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

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

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <b>Ambulatory /Inpatient</b>	HITSC Privacy and Security Workgroup Recommendations	
			Recommended New or Revised Certification Criterion	Recommended Standard(s) and/or Implementation Specification(s)
37	<p>(continued) Perform, or update, security risk assessment and address deficiencies.</p> <p>Address encryption for data at rest. EPs and EHs attest to this policy.</p>	<p>§ 170.302(r)</p> <p><u>Audit log.</u> (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in § 170.210(b). (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).</p>	<p><u>Activity auditing.</u> (1) <u>Detect and record auditable events.</u> (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). (2) <u>Protect audit information.</u> (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.</p> <p><u>Generate audit report(s).</u> 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).</p>	<p>STANDARD: Record audit data about security-relevant events.</p> <p>IMPLEMENTATION SPEC: ASTM E2147-01, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems;</p>

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

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

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <b>Ambulatory /Inpatient</b>	HITSC Privacy and Security Workgroup Recommendations	
			Recommended New or Revised Certification Criterion	Recommended Standard(s) and/or Implementation Specification(s)
40	<p>(continued) Perform, or update, security risk assessment and address deficiencies.</p> <p>Address encryption for data at rest. EPs and EHs attest to this policy.</p>	<p>§ 170.302(u)</p> <p><u>General encryption.</u> 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.</p>	<p><u>General encryption.</u> EHR must be able to encrypt and decrypt electronic health information in accordance with the standard specified in §170.210(a)(1).</p> <p>(1) <u>Data-at-rest encryption.</u> 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.</p>	<p>STANDARD: FIPS Pub 140-2, Annex A [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]</p> <p>IMPLEMENTATION SPEC: NIST SP 800-111</p>
41		<p>§ 170.302(v)</p> <p><u>Encryption when exchanging electronic health information.</u> Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).</p>	<p>(2) <u>Encryption when exchanging electronic health information.</u> EHR technology must assure that all health information exchanged with external entities is encrypted and integrity-protected.</p>	<p>STANDARDS: FIPS Pub 140-2, Annex A; IETF RFC 2246 (TLS 1.0); IETF RFC 2401 (IPsec)</p> <p>IMPLEMENTATION SPEC: NIST SP 800-52 (TLS); NIST SP 800-77 (IPsec VPN); NIST SP 800-113 (SSL VPN); other transport or network layer protocols validated i.a.w. FIPS Pub 140-2</p> <p>NwHIN transport standards</p>

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <i>Ambulatory /Inpatient</i>	HITSC Privacy and Security Workgroup Recommendations	
			Recommended New or Revised Certification Criterion	Recommended Standard(s) and/or Implementation Specification(s)
42	(continued) Perform, or update, security risk assessment and address deficiencies.  Address encryption for data at rest. EPs and EHs attest to this policy.	§ 170.302(w) <i>Optional</i>  <u>Accounting of disclosures</u> . 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  (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  (NEW) 2-Factor Authentication For Controlled Substances (Providers)		[P&S WG agrees with Implementation WG – out of scope]	
45	Privacy and Security  (NEW) Entity Level Digital Certificates (Providers)		[P&S WG agrees with Implementation WG – out of scope]	

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <b>Ambulatory /Inpatient</b>	HITSC Privacy and Security Workgroup Recommendations	
			Recommended New or Revised Certification Criterion	Recommended Standard(s) and/or Implementation Specification(s)
51	Privacy and Security  <b>(NEW)</b> 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)		<p><b>[COMMENT:</b> In considering the potential implications of this policy for EHR technology, the P&amp;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.]</p>	

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

IWG Ref	HITPC Proposed MU Stage 2 Objective/Measure & Direction to HITSC	Stage 1 Adopted Certification Criterion <b>Ambulatory /Inpatient</b>	HITSC Privacy and Security Workgroup Recommendations	
			Recommended New or Revised Certification Criterion	Recommended Standard(s) and/or Implementation Specification(s)
52	<p>Amendments</p> <p><b>(NEW)</b> CEHRT should make it technically possible for providers to:</p> <p>(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)</p> <p>(2) Append information from the patient and any rebuttal from the entity regarding disputed data</p>		<p>(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.</p> <p>(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.</p> <p>(3) EHR must maintain an audit trail of the amendments to health information (1 and 2 above).</p>	

## GENERAL PRIVACY AND SECURITY RECOMMENDATIONS

### 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