Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	
S1	Sec	Security: Access Control	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.	ISO 17799: 9.1.1.2.b; HIPAA: 164.312(a)(1)	**P**			

S2			The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.	Canadian: Alberta 4.1.3 (EMR);
				CC SFR: FMT_MSA;
				SP800-53: AC-5 LEAST PRIVILEGE;
				HIPAA: 164.312(a)(1)
					P			

S3			The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role-based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)	Canadian: Ontario 5.3.12.e (System Access Management);
				CC SFR: FDP_ACC, FMT_MSA;
				ASTM: E1985-98;
				SP800-53: AC-3 ACCESS AND INFORMATION FLOW CONTROL;
				HIPAA: 164.312(a)(1)
					P			

S4			The system shall support removal of a user's privileges without deleting the user from the system. The purpose of the criteria is to provide the ability to remove a user's privileges, but maintain a history of the user in the system.		**M**			
S5.1	Sec	Security: Audit	**Removed**		**M**			

S5.2			The system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session timeout, account lockout, patient record created/viewed/updated/deleted, scheduling, query, order, node-authentication failure, signature created/validated, PHI export (e.g. print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.	CC SFR: FAU_GEN;
				SP800-53: AU-2 AUDITABLE EVENTS;
				HIPAA: 164.312(b)
					M			

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	

S6			The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.	CC SFR: FAU_GEN;
				SP800-53: AU-3 CONTENT OF AUDIT RECORDS, AU-10 NON-REPUDIATION;
				HIPAA: 164.312(b)
					P			

S7			The system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. UTC synchronization).	CC SFR: FAU_SAR;
				SP800-53: AU-7 AUDIT REDUCTION AND REPORT GENERATION;
				HIPAA: 164.312(b)
					M			

S8.1			The system shall be able to support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.	CC SFR: FPT_STM; SP800-53: AU-8 TIME STAMPS	**P**			
S8.2			The system shall have the ability to format for export recorded time stamps using UTC based on ISO 8601. Example: "1994-11-05T08:15:30-05:00" corresponds to November 5, 1994, 8:15:30 am, US Eastern Standard Time.	CC SFR: FPT_STM; SP800-53: AU-8 TIME STAMPS	**M**			

S9			The system shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall prevent modifications to the audit records.	CC SFR: FAU_SAR, FAU_STG;
				SP800-53: AU-9 PROTECTION OF AUDIT INFORMATION;
				HIPAA: 164.312(a)(1)
					P			

S10			**Removed**		**M**			

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	
S11			The system shall allow an authorized administrator to enable or disable auditing for groups of related events to properly collect evidence of compliance with implementation-specific policies. Note: In response to a HIPAA-mandated risk analysis and management, there will be a variety of implementation-specific organizational policies and operational limits.	CC SFR: FAU_SEL; HIPAA 164.312(b)	**M**			

S12	Sec	Security: Authentication	The system shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed, including when not connected to a network e.g. mobile devices.	Canadian: Alberta 1.1;
				CC SFR: FIA_UAU, FIA_UID;
				SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION;
				HIPAA: 164.312(d)
					P			

S13			When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.	Canadian: Alberta 7.3.12 (Security)
				Canadian Ontario 5.3.12.b (System Access Management);
				CC SFR: FIA_SOS, FIA_UAU, FIA_UID;
				ASTM: E1987-98;
				SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION (no strength of password);
				ISO 17799: 9.3.1.d;
				HIPAA: 164.
					P			

S14			The system upon detection of inactivity of an interactive session shall prevent further viewing and access to the system by that session by terminating the session, or by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.	Canadian: Alberta 7.3.14 (Security)
				Canadian Ontario 5.6.12.a (Workstation Security);
				CC SFR: FTA_SSL, FMT_SAE;
				SP800-53: AC-11 SESSION LOCK;
				HIPAA: 164.312(a)(1)
					M			

S15			The system shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The system shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).	Canadian: Ontario 5.3.12.c (System Access Management);
				CC SFR: FIA_AFL, FMT_SAE;
				SP800-53: AC-6 UNSUCCESSFUL LOGIN ATTEMPTS, AC-11 SESSION LOCK ;
				ISO 17799: 9.3.1.e, 9.5.2.e;
				HIPAA: 164.312(a)(1)
					M			

S16.1			When passwords are used, the system shall provide an administrative function that resets passwords.	CC SFR: FMT_MTD;
				ISO 17799: 9.2.3.b, (9.3.1.f);
				HIPAA: 164.312(d)
					P			

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	

S16.2			When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.	CC SFR: FMT_MTD;
				ISO 17799: 9.2.3.b, (9.3.1.f);
				HIPAA: 164.312(d)
					P			

S17			The system shall provide only limited feedback information to the user during the authentication.	CC SFR: FIA_UAU;
				SP800-53: IA-6 AUTHENTICATOR FEEDBACK;
				HIPAA: 164.312(d)
					P			

S18			The system shall support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).	CC SFR: FMT_MTD	**P**			
S19			When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rules (S13).	CC SFR: FMT_MTD	**P**			
S20			When passwords are used, the system shall support case-sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).	Canadian: Ontario 5.3.12 (b); SP 800-63	**P**			
S21			When passwords are used, the system shall not store passwords in plain text.		**P**			

S22			When passwords are used, the system shall prevent the reuse of passwords previously used within a specific (configurable) timeframe (i.e., within the last X days, etc. - e.g. "last 180 days"), or shall prevent the reuse of a certain (configurable) number of the most recently used passwords (e.g. "last 5 passwords").	CC SFR: FMT_MTD;
				ISO 17799 9.5.4.f;
				HIPAA 164.312(d)
					M			

S23	Sec	Security: Documentation	The system shall include documentation available to the customer that provides guidelines for configuration and use of the EHR security controls necessary to support secure and reliable operation of the system, including but not limited to: creation, modification, and deactivation of user accounts, management of roles, reset of passwords, configuration of password constraints, and audit logs.	CC SFR: AGD_ADM	**M**			

S24	Sec	Security: Technical Services	The system shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPSec, XML encryptions, or S/MIME or their successors.	Canadian: Alberta 7.4.6.2 & 8.4.6.2 (Technical);
				CC SFR: FCS_COP;
				SP800-53: SC-13 CRYPTOGRAPHIC OPERATIONS;
				HIPAA: 164.312(e)(1)
					P			

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	

S25			When passwords are used, the system shall not transport passwords in plain text.	Canadian: Ontario 5.3.12.a (System Access Management);
				CC SFR: FCS_CKM;
				SP800-53: SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT;
				HIPAA: 164.312(e)(1)
					P			

S26			When passwords are used, the system shall not display passwords while being entered.	CC SFR: FPT_ITC;
				ISO 17799 9.2.3;
				HIPAA 164.312(a)(1)
					P			

S27			For systems that provide access to PHI through a web browser interface (i.e. HTML over HTTP) shall include the capability to encrypt the data communicated over the network via SSL (HTML over HTTPS). Note: Web browser interfaces are often used beyond the perimeter of the protected enterprise network	CC SFR: AGD_ADM	**P**			
S28			The system shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.	CC SFR: FPT_RCV	**P**			
S29			The system shall support ensuring the authenticity of remote nodes (mutual node authentication) when communicating Protected Health Information (PHI) over the Internet or other known open networks using an open protocol (e.g. TLS, SSL, IPSec, XML sig, S/MIME).	CC SFR: FPT_RCV	**P**			
S30	Sec		The system, when storing PHI on any physical media intended to be portable/removable (e.g. thumb-drives, CD-ROM, PDA), shall support use of a standards based encrypted format using triple-DES (3DES), and the Advanced Encryption Standard (AES).	FIPS 140-2, CC SFR: FCS_COP, OMB M-06-16			N	
S31	Sec	Security: Authentication	The system shall support two-factor authentication in alignment with NIST 800-63 Level 3 Authentication. Note: The standards in this area are still evolving.	CC SFR: FIA_UAU; SP800-53: IA-2/AC-19, OMB M-06-16			N	
S32	Sec	Security: Technical Services	The system shall support the storage of any Protected Health Information (PHI) data on any associated mobile device(s) such as PDAs, smartphones, etc. in an encrypted format, using triple-DES (3DES), the Advanced Encryption Standard (AES), or their successors.	FIPS 140-2, CC SFR: FCS_COP, OMB M-06-16, SP800-53: AC-19			N	

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	
S33	Sec		The system, prior to a user login, shall display a (configurable) notice warning (e.g. "The system should only be accessed by authorized users").	CC 2.1 L.4 TOE access banners (FTA_TAB); CC 3.0 FIA_TIN.1 Advisory warning message			N	
S34	Sec	Security: Access Control	The system shall allow certain role clinicians to mark a patient's specific information as blinded, prohibiting access to all other users. Note: The standards in this area are still evolving.	§164.312(a)(2)(ii)		N		
S35	Sec		The system shall support access to blinded information to a treating clinician, when the blinded information is necessary for managing an emergency condition. Note: This is commonly known as a "break the glass" function. This does not provide increased access rights for the user.	§164.312(a)(2)(ii)		N		
S36	Sec		The "break the glass" function must be capable of requiring the clinician requesting access to blinded information to document and record the reason(s) for requesting access.	§164.312(a)(2)(ii)		N		
S37	Sec	Security: Audit	The system shall support logging to a common audit engine using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile	NIST 800-92/SP 800-92			N	

R1	Sec	Reliability: Backup / Recovery	The system shall be able to generate a backup copy of the application data, security credentials, and log/audit files.	Canadian: Alberta 7.3.16 (Security);
				CC SFR: FDP_ROL, FPT_RCV;
				HIPAA: 164.310(d)(1)
					P			

R2			The system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.	Canadian: Alberta 7.3.18.9 (Security);
				CC SFR: FAU_GEN;
				SP800-53: AU-2 AUDITABLE EVENTS;
				HIPAA: 164.310(d)(1)
					P			

R3			If the system claims to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.	Canadian: Alberta 7.4.2.5 (Technica+D1l);
				CC SFR: FDP_ROL;
				HIPAA: 164.310(d)(1)
					P			

R4	Sec	Reliability: Documentation	The system shall include documentation available to the customer stating whether or not there are known issues or conflicts with security services in at least the following serivce areas: antivirus, intrusion detection, malware eradication, host-based firewall and the resolution of that conflict (e.g. most systems should note that full virus scanning should be done outside of peak usage times and should exclude the databases.).	Canadian: Alberta 7.3.17 (Security);
				CC SFR: FPT_TST
				CC SFR: AGD_ADM;
				SP800-53 SI-3 MALICIOUS CODE PROTECTION
					M			

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	
R5			If the system includes hardware, the system shall include documentation that covers the expected physical environment necessary for proper secure and reliable operation of the system including: electrical, HVAC, sterilization, and work area.	CC SFR: AGD_ADM	M			
R6			**Removed**					

R7			The system shall include documentation that itemizes the services (e.g. PHP, web services) and network protocols/ports (e.g. HL-7, HTTP, FTP) that are necessary for proper operation and servicing of the system, including justification of the need for that service and protocol. This information may be used by the healthcare facility to properly configure their network defenses (firewalls and routers).	CC SFR: AGD_ADM;
				SP 800-53 AC-5 CM-6;
				SP 800-70;
				HIPAA 164.312(a)(1)
					M			

R8			**Removed (Merged with R4)**					
R9			The system shall include documentation that describes the steps needed to confirm that the system installation was properly completed and that the system is operational.	CC SFR: AGD_ADM	M			
R10			The system shall include documentation that describes the patch (hot-fix) handling process the vendor will use for EHR, operating system and underlying tools (e.g. a specific web site for notification of new patches, an approved patch list, special instructions for installation, and post-installation test).	CC SFR: AGD_ADM	M			
R11			The system shall include documentation that explains system error or performance messages to users and administrators, with the actions required.	CC SFR: AGD_ADM	P			
R12			The system shall include documentation of product capacities (e.g. number of users, number of transactions per second, number of records, network load, etc.) and the baseline representative configurations assumed for these capacities (e.g. number or type of processors, server/workstation configuration and network capacity, etc).	CC SFR: AGD_ADM; SP800-53 CM-2	M			
R13			The system shall include documented procedures for product installation, start-up and/or connection.	CC SFR: ADO_IGS	P			

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	
R14	Sec	Reliability: Technical Services	The software used to install and update the system, independent of the mode or method of conveyance, shall be certified free of malevolent software ("malware"). Vendor may self-certify compliance with this standard through procedures that make use of commercial malware scanning software.	CC SFR: ADO_DEL	M			
R15			**Removed**					
R16	Sec	Reliability: Documentation	The system shall include documentation of the minimal privileges necessary for each service and protocol necessary to provide EHR functionality and/or serviceability.	SP800-53 AC-5	P			
R17	Sec	Reliability: Technical Services	The system shall be configurable to prevent corruption or loss of data already accepted into the system in the event of a system failure (e.g. integrating with a UPS, etc.).	CC SFR: FPT_RCV	P			
R18	Sec		**Removed (Merged with S23)**					
R19			**Removed**					

References:
1) ISO 17799: ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management. http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

2) HIPAA: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996. 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf

3) Alberta VCUR Standards: Alberta Medical Association, Vendor Conformance and Usability Requirements (VCUR), April 18, 2006. http://www.posp.ab.ca/vendors/VCURv2.asp

4) CC SFR: (Common Criteria for Information Technology Security Evaluations - Part 2: Security functional requirements) - ISO/IEC 15408:2005-2 Security Techniques—Evaluation Criteria for IT Security is based on Common Criteria for Information Technology Security Evaluation 2.3 (referred to as Common Criteria or CC).
http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm

5) NIST 800-53 - Recommended Security Controls for Federal Information Systems ;800-63 - Electronic Authentication Guideline;800-70 - Security
Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers;800-92 - Guide to Computer Security Log Management. http://csrc.nist.gov/publications/nistpubs/

*Assignable Functions:
Applicants may assign certain functionality to a third party (e.g. when security and operating functions are handled by the operating system, a third party component, tool or service, etc.). Where a function is indicated as "assignable", applicants can indicate they are delegating and provide related materials for self attestation. For example – for backup and restore: applicants that use a third party database backup utility could assign backup functionality and provide related documentation for self-attestation.

Security - 2007 Final Criteria - Mar 16 2007

Final Secuirty Criteria For 2007 Certification of EHRs

Legend:
Provisional Criteria (2007) are highlighted in yellow
P= Previous
N= New
M= Modified

Line #	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.	Compliance			Discussion/Comments
					Certify in May 2007	Roadmap for May 2008	Roadmap for May 2009 and beyond	
6) Ontario specification references are from: Ontario Medical Association, CMS Local Solution Specification V1.3. Copy located at: http://www.ontariomd.ca/cms/infoForVendors.shtml								