



Ambulatory Certification Criteria
2008 Final Criteria
 May 13, 2008

© 2008 The Certification Commission for Healthcare Information Technology

2008 Criteria #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	Test Script Reference	Internal WG #
						2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond				
SC 01.01	SC	FN	1. Access Control	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.	P			Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year O = Provisional	ISO 17799: 9.1.1.2.b; HIPAA: 164.312(a)(1)	5.13, 5.14, 5.20, 5.23	S1
SC 01.02	SC	FN	1. Access Control	Security Access Control	The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.	P				Canadian: Alberta 4.1.3 (EMR); CC SFR: FMT_MSA; SP800-53: AC-5 LEAST PRIVILEGE; HIPAA: 164.312(a)(1)	5.18	S2
SC 01.03	SC	FN	1. Access Control	Security Access Control	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.)	P				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)	5.10, 5.13, 5.14, 5.18, 5.20, 5.23	S3
SC 01.04	SC	FN	1. Access Control	Security Access Control	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.	P					5.39, 5.41, 5.42, 5.44, 5.46, 5.47	S4
SC 01.05	SC	FN	1. Access Control	Security: Access Control	If role-based access control (RBAC) is supported, the system shall be able to provide role based access control that is in compliance with the HL7 Permissions Catalog.			N		HL7 Permissions Catalog		S40
SC 01.06	SC	FN	1. Access Control	Security: Access Control	If role-based access control (RBAC) is supported, the system must be capable of operating within an RBAC infrastructure conforming to ANSI INCITS 359-2004, American National Standard for Information Technology – Role Based Access Control.			N		ANSI INCITS 359-2004, American National Standard for Information Technology - Role Based Access Control		S41

2008 Criteria #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	Test Script Reference	Internal WG #
						2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond				
SC 02.01	SC	FN	2. Audit	Security Audit	The system shall allow an authorized administrator to enable or disable auditing for events or 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.		P		This criterion was provisional for 2007 and is being moved to 2009 Roadmap for revision based on an analysis of 2008 pilot test results and commission's recommendations on 4/15/2008.	CC SFR: FAU_SEL; HIPAA 164.312(b)		S11
SC 02.03	SC	FN	2. Audit	Security Audit	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.		P			CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.312(b)	5.51	S5.2
SC 02.04	SC	FN	2. Audit	Security Audit	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.		P			CC SFR: FAU_GEN; SP800-53: AU-3 CONTENT OF AUDIT RECORDS, AU-10 NON-REPUDIATION; HIPAA: 164.312(b)	5.52	S6
SC 02.05	SC	FN	2. Audit	Security Audit	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).		P		Assignable to third party.	CC SFR: FAU_SAR; SP800-53: AU-7 AUDIT REDUCTION AND REPORT GENERATION; HIPAA: 164.312(b)	5.52, 7.14	S7
SC 02.06	SC	FN	2. Audit	Security Audit	The system shall be able to support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.		P		Assignable to third party.	CC SFR: FPT_STM; SP800-53: AU-8 TIME STAMPS	6.12, 7.18	S8.1

Compliance Key:
P = Previous Criteria
M = Modified for Year
N = New for Year
O = Provisional

2008 Criteria #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	Test Script Reference	Internal WG #
						2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond				
SC 02.07	SC	FN	2. Audit	Security Audit	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.	O			This criterion was provisional for 2007 and will continue to be provisional in 2008 due to a change made to test step based on 2008 pilot test results.	CC SFR: FPT_STM; SP800-53: AU-8 TIME STAMPS	5.53	S8.2
SC 02.08	SC	FN	2. Audit	Security Audit	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.	P			This criterion is being changed to be an assignable criteria for 2008	CC SFR: FAU_SAR, FAU_STG; SP800-53: AU-9 PROTECTION OF AUDIT INFORMATION; HIPAA: 164.312(a)(1)	5.14, 5.20	S9
SC 03.01	SC	FN	3. Authentication	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.	P			Assignable to third party.	Canadian: Alberta 1.1; CC SFR: FIA_UAU, FIA_UID; SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION; HIPAA: 164.312(d)	5.18, 5.22, 5.29, 5.34, 5.36, 5.41, 7.09	S12
SC 03.02	SC	FN	3. Authentication	Security Authentication	When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.	P			Assignable to third party.	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.	5.11, 5.26, 5.30, 7.05, 7.13	S13
SC 03.03	SC	FN	3. Authentication	Security Authentication	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.	P			Assignable to third party.	Canadian: Alberta 7.3.14 (Security) Canadian Ontario 5.6.12.a (Workstation Security); CC SFR: FIA_SSL, FMT_SAE; SP800-53: AC-11 SESSION LOCK; HIPAA: 164.312(a)(1)	5.25, 5.28, 5.29, 7.12	S14
SC 03.04	SC	FN	3. Authentication	Security Authentication	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).	P			Assignable to third party.	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)	5.12, 5.32, 5.33, 5.34, 7.06	S15

2008 Criteria #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	Test Script Reference	Internal WG #
						2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond				
SC 03.05	SC	FN	3. Authentication	Security Authentication	When passwords are used, the system shall provide an administrative function that resets passwords.	P			Assignable to third party.	CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)	5.50, 7.15	S16.1
SC 03.06	SC	FN	3. Authentication	Security Authentication	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.	P			Assignable to third party.	CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)	5.55, 7.16	S16.2
SC 03.07	SC	FN	3. Authentication	Security Authentication	The system shall provide only limited feedback information to the user during the authentication.	P			Assignable to third party.	CC SFR: FIA_UAU; SP800-53: IA-6 AUTHENTICATOR FEEDBACK; HIPAA: 164.312(d)	5.17, 5.19, 5.42, 7.08	S17
SC 03.08	SC	FN	3. Authentication	Security Authentication	The system shall support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).	P			Assignable to third party.	CC SFR: FMT_MTD	5.22, 7.11	S18
SC 03.09	SC	FN	3. Authentication	Security Authentication	When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rules (SC 03.02).	P			Assignable to third party.	CC SFR: FMT_MTD	5.26, 5.30, 7.13	S19
SC 03.10	SC	FN	3. Authentication	Security Authentication	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).	P			Assignable to third party.	Canadian: Ontario 5.3.12 (b); SP 800-63	5.16, 5.18, 5.22, 7.07	S20
SC 03.11	SC	FN	3. Authentication	Security Authentication	When passwords are used, the system shall use either standards-based encryption, e.g., 3DES, AES, or standards-based hashing, e.g., SHA1 to store or transport passwords.	M				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)	6.17, 6.18, 7.23, 7.24	S21
SC 03.12	SC	FN	3. Authentication	Security Authentication	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").	P			Assignable to third party.	CC SFR: FMT_MTD; ISO 17799 9.5.4.f; HIPAA 164.312(d)	6.01, 7.25	S22
SC 03.13	SC	FN	3. Authentication	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.			M		CC SFR: FIA_UAU; SP800-53: IA-2/AC-19, OMB M-06-16		S31
SC 04.01	SC	FN	4. Documentation	Reliability: Documentation	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).	P				CC SFR: AGD_ADM	6.07	R10

2008 Criteria #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	Test Script Reference	Internal WG #
						2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond				
SC 04.02	SC	FN	4. Documentation	Reliability: Documentation	The system shall include documentation that explains system error or performance messages to users and administrators, with the actions required.	P				CC SFR: AGD_ADM	6.08	R11
SC 04.03	SC	FN	4. Documentation	Reliability: Documentation	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).	P				CC SFR: AGD_ADM; SP800-53 CM-2	6.09	R12
SC 04.04	SC	FN	4. Documentation	Reliability: Documentation	The system shall include documented procedures for product installation, start-up and/or connection.	P				CC SFR: ADO_IGS	6.06	R13
SC 04.05	SC	FN	4. Documentation	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.	P				SP800-53 AC-5	6.05	R16
SC 04.06	SC	FN	4. Documentation	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 service 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.).	P				Canadian: Alberta 7.3.17 (Security); CC SFR: FPT_TST CC SFR: AGD_ADM; SP800-53 SI-3 MALICIOUS CODE PROTECTION	6.03	R4□
SC 04.07	SC	FN	4. Documentation	Reliability: Documentation	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.	P				CC SFR: AGD_ADM	6.04	R5
SC 04.08	SC	FN	4. Documentation	Reliability: Documentation	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).	P				CC SFR: AGD_ADM; SP 800-53 AC-5 CM-6; SP 800-70; HIPAA 164.312(a)(1)	6.05	R7□
SC 04.09	SC	FN	4. Documentation	Reliability: Documentation	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.	P				CC SFR: AGD_ADM	6.06	R9

Compliance Key:
P = Previous Criteria
M = Modified for Year
N = New for Year
O = Provisional

2008 Criteria #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	Test Script Reference	Internal WG #
						2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond				
SC 04.10	SC	FN	4. Documentation	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.	P			Assignable to third party.	CC SFR: AGD_ADM	5.04, 5.09, 6.02, 7.04	S23
SC 05.01	SC	FN	5. Technical Services	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.	P				CC SFR: ADO_DEL	6.11	R14
SC 05.02	SC	FN	5. Technical Services	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.).	P			Assignable to third party.	CC SFR: FPT_RCV	6.10, 7.17	R17
SC 06.01	SC	FN	6. Technical Services	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.	P			Assignable to third party.	Canadian: Alberta 7.4.6.2 & 8.4.6.2 (Technical); CC SFR: FCS_COP; FIPS 140-2; SP800-53: SC-13 CRYPTOGRAPHIC OPERATIONS; HIPAA: 164.312(e)(1); HITSP T17,	6.13, 7.19	S24
SC 06.02	SC	FN	6. Technical Services	Security Technical Services	When passwords are used, the system shall not display passwords while being entered.	P			Assignable to third party.	CC SFR: FPT_ITC; ISO 17799 9.2.3; HIPAA 164.312(a)(1)	5.19, 7.10	S26
SC 06.03	SC	FN	6. Technical Services	Security Technical Services	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	P			Assignable to third party.	CC SFR: AGD_ADM	6.16, 7.22	S27
SC 06.04	SC	FN	6. Technical Services	Security Technical Services	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.	P			Assignable to third party.	CC SFR: FPT_RCV; FIPS 140-2; SP800-53: SC-13 CRYPTOGRAPHIC OPERATIONS; HIPAA: 164.312(e)(1); HITSP T17	6.14, 7.20	S28
SC 06.05	SC	FN	6. Technical Services	Security Technical Services	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).	P			Assignable to third party.	CC SFR: FPT_RCV; HITSP T17	6.15, 7.21	S29

2008 Criteria #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	Test Script Reference	Internal WG #
						2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond				
SC 06.07	SC	FN	6. Technical Services	Security: Technical Services	The system, prior to a user login, shall display a (configurable) notice warning (e.g. "The system should only be accessed by authorized users").		P			CC 2.1 L.4 TOE access banners (FTA_TAB); CC 3.0 FIA_TIN.1 Advisory warning message		S33
SC 07.01	SC	FN	7. Inter-Domain	Security: Inter Domain	The system shall be able to communicate identity information across domains and web services using standards based user authentication and access control.			N		HITSP/C19, ANSI INCITS 359-2004, American National Standard for Information Technology - Role Based Access Control		S38
SC 07.02	SC	FN	7. Inter-Domain	Security: Inter Domain	When the system uses HITSP TP13 (IHE XDS) as a Document Consumer, the system shall be able to use the TP13 "Document Integrity" option. This may be a configurable parameter or may be enabled at all times			N		HITSP TP13 (IHE XDS)		S39
SC 08.01	SC	FN	8. Backup/Recovery	Reliability: Backup and Recovery	The system shall be able to generate a backup copy of the application data, security credentials, and log/audit files.	P			Assignable to third party.	Canadian: Alberta 7.3.16 (Security); CC SFR: FDP_ROL, FPT_RCV; HIPAA: 164.310(d)(1)	5.01, 7.01	R1
SC 08.02	SC	FN	8. Backup/Recovery	Reliability: Backup and Recovery	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.	P			Assignable to third party.	Canadian: Alberta 7.3.18.9 (Security); CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.310(d)(1)	5.06, 5.08, 7.03	R2
SC 08.03	SC	FN	8. Backup/Recovery	Reliability: Backup and Recovery	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.	P			Assignable to third party.	Canadian: Alberta 7.4.2.5 (Technica+D11); CC SFR: FDP_ROL; HIPAA: 164.310(d)(1)	5.02, 7.02	R3