CCHIT-IFR Stage 1 Certification Criteria Gap Analysis - Security Criteria

(Applies to Eligible Providers and Hospitals)

IFR Criteria	Preliminary ARRA 2011 Criteria	Gap: IFR vs Preliminary ARRA 2011	Gap: IFR vs Comprehensive 2011
1. 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.	Provide capability to assign a unique name and/or number for identifying and tracking user identity. (AR.FND 01.02)	No retesting needed	No retesting needed
	Provide capability to allow access only to those persons or software programs that have been granted access rights. (AR.FND 01.01)		
2. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	Provide capability to access necessary electronic protected health information during an emergency. (AR.FND 01.03)	No retesting needed	No retesting needed
3. Terminate an electronic session after a predetermined time of inactivity.	Provide capability to terminate an electronic session after a predetermined time of inactivity. (AR.FND 01.04)	No retesting needed	No retesting needed
4. Encrypt and decrypt electronic health information according to user-defined preferences (e.g., backups, removable media, at log-on/off) in accordance with the standard specified in Table 2B row 1.	Provide the capability to encrypt and decrypt electronic protected health information. (AR.FND 01.05)	No retesting needed	No retesting needed
	Provide the capability to encrypt data at rest using AES. (AR.FND 01.06)		
5. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in Table 2B row 2.	Provide the capability to use AES to encrypt data for transmission.(AR.FND 08.05)	No retesting needed (requirements simplified)	No retesting needed (requirements simplified)
	Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. (AR.FND 08.03)		
	Provide the capability to use TLS (with SHA-2 and AES) to establish a mutually authenticated, encrypted, and integrity-protected channel for data exchanges over the World Wide Web. (AR.FND 08.06)		
	If an email capability is provided, implement the CMS standard to cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption. (AR.FND 08.07)		

6. Record actions (e.g., deletion) related to electronic health information in accordance with the standard specified in Table 2B row 3 (i.e., audit log), provide alerts based on user-defined events, and electronically display and print all or a specified set of recorded information upon request or at a set period of time.	Provide the capability to record and examine activity in information systems that contain or use electronic protected health information. (AR.FND 02.01)	No retesting needed	No retesting needed
	Provide the capability to use the ATNA profile to communicate audit messages between Secure Nodes and to establish Audit Repository nodes to collect audit information. (AR.FND 02.02)		
7. Verify that electronic health information has not been altered in transit and detect the alteration and deletion of electronic health information and audit logs in accordance with the standard specified in Table 2B row 4.	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (AR.FND 08.01)	No retesting needed	No retesting needed
	Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. (AR.FND 08.02)		
	Provide the capability to use SHA to protect the integrity of data transmissions. (AR.FND 08.04)		
8. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.	Person or entity authentication: Provide the capability to verify that a person or entity seeking access to electronic protected health information is the one claimed. (AR.FND 03.01)	No retesting needed (Kerberos and EUA requirements dropped)	*No retesting needed (Kerberos and EUA requirements dropped)*
	Provide the capability to authenticate users and entities within an organization using Kerberos. (AR.FND 03.02)		
	Implement the EUA Profile (which uses Kerberos) to provide a single sign-on capability within enterprises. (AR.FND 03.03)		
9. Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in Table 2B row 5.		Retest needed IF the technology performs cross-enterprise user authentication	Retest needed IF the technology performs cross-enterprise user authentication

10. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in Table 2B row 6.r	Provide the capability to electronically record individual consumers' consents and authorizations. (AR.FND 04.01)	Retest needed IF the technology discloses information for treatment, payment, and health care operations	Retest needed IF the technology discloses information for treatment, payment, and health care operations
Criteria below are either covered elsewhere or dropped from the IFR criteria			
	Provide the capability to create an electronic copy of an individual's electronic health record, to record it on removable media, and to transmit it to a designated entity capable of receiving electronic transmissions. (AR.FND 05.01)	No retesting needed (covered elsewhere)	No retesting needed (covered elsewhere)
	Provide the capability to create and distribute an electronic copy of an individual's EHR as an unstructured document. (AR.FND 05.02)	No retesting needed (covered elsewhere)	No retesting needed (covered elsewhere)
	Provide the capability to remove the identifiers enumerated in Section 164.514(b)(2)(i) of the HIPAA Privacy Rule. (AR.FND 06.01)	No retesting needed (dropped)	No retesting needed (dropped)
	Provide the capability to generate and assign a code or other means of record identification to allow information de-identified in accordance with the HIPAA Privacy Rule to be re-identified by the covered entity; such code or other means must not be derived from or related to the information and must not be otherwise capable of being translated so as to disclose the identity of the individual. (AR.FND 06.02)	No retesting needed (dropped)	No retesting needed (dropped)
	Provide the capability to protect the code or other means of record identification from unauthorized disclosure. (AR.FND 06.03)	No retesting needed (dropped)	No retesting needed (dropped)
	Use ISO/TS 25237 as guidance in the implementation of pseudonymization capabilities. (AR.FND 06.04)	No retesting needed (dropped)	No retesting needed (dropped)
	Provide the capability to protect electronic protected health information from improper alteration or destruction. (AR.FND 07.01)	No retesting needed (covered elsewhere)	No retesting needed (covered elsewhere)

	Provide electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. (AR.FND 07.02)	No retesting needed (covered elsewhere)	No retesting needed (covered elsewhere)
	Provide the capability to use SHA to protect the integrity of data at rest. (AR.FND 07.03)	No retesting needed (covered elsewhere)	No retesting needed (covered elsewhere)
	Use as guidance in the design and implementation of electronic signatures. (AR.FND 07.04)	No retesting needed (covered elsewhere)	No retesting needed (covered elsewhere)