CCHIT℠
Certification Commission
for Health Information
Technology

Security Test Script Guidance

For Preliminary ARRA IFR Stage 1 Certification EHR Technology

April 7, 2010

Product (NUMBER CODE ONLY):_________________________ Date: __________________________

Evaluator: ____ Signature: _______________________

FOUNDATIONAL INFRASTRUCTURE: Security and Privacy (MU.P5.G1)

All test steps must be demonstrated. The applicant explicitly attests to the veracity of the features and functions demonstrated, the information furnished, and the statements made during the course of this inspection.

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.01	Demonstrate and describe how the technology provides the capability to 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.	The capability is demonstrated.	IFR.01 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.	There are multiple ways you might demonstrate compliance with this step, including: 1. Uniqueness of user IDs 2. Composition of user IDs 3. Case sensitivity and case insensitivity of user IDs 4. The ability to provide access only to authenticated users 5. The authentication procedure (e.g. account creation including user IDs, assignment of privileges, 6. The access control method, user-based, RBAC, SSO, EUA, SAML, context-based, etc. 7. The product’s password strength rule and password security (age, reuse, display, encryption, etc.) 8. The product’s limit of number of consecutive invalid attempt 9. The product’s account lockout after exceeding the limit of number of invalid attempt: - configurable time delay until next login attempt - require release by administrator 10. The ability to suspend user accounts 11. The history of inactive accounts 12. The ability to configure and display notice of warning against unauthorized use 13. The ability to track user IDs in audit records 14. The ability to generate audit records for valid logins and invalid login attempts with user IDs

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.02	Demonstrate and describe how the technology provides the capability to permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	The capability is demonstrated.	IFR.02 Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	There are multiple ways you might demonstrate compliance with this step, including: 1. The support for emergency access policies 2. The method supported for clinical user access in emergency situations, also known as the “break the glass” function 3. The support for the expiration of emergency mode 4. Audit events tracking the start of emergency mode and the users using the emergency mode. 5. Removal of the access emergency privileges upon the expiration of emergency.
FND.03	Demonstrate and describe how the technology provides the capability to terminate an electronic session after a predetermined time of inactivity.	The capability is demonstrated.	IFR.03 Terminate an electronic session after a predetermined time of inactivity.	There are multiple ways you might demonstrate compliance with this step, including: 1. The ability to configure the period of inactivity for timeout 2. The ability to prevent further access 3. The ability to prevent further display of information 4. The ability to re-authenticate after inactivity timeout

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.04	Demonstrate and describe how the technology provides the capability to encrypt and decrypt electronic protected 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.	The capability is demonstrated.	IFR.04 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. ***Table 2B row 1 General Encryption and Decryption of Electronic Health Information:*** A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used (e.g., FIPS 197 Advanced Encryption Standard, (AES), Nov 2001).	There are multiple ways you might demonstrate compliance with this step, including: 1. Identify the encryption method and the software and/or hardware tools used for standards based encryption 2. Demonstrate the availability (license) of the encryption software 3. Demonstrate access to the tools and available encryption/decryption algorithms 4. Demonstrate the availability of the procedure to encrypt and decrypt PHI 5. Demonstrate the menus, functions, options and the choice for selecting or implementing the methods identified above 6. Identify the media or the location of data at rest.

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.05	Demonstrate and describe how the technology provides the capability to encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in Table 2B row 2.	The capability is demonstrated.	IFR.05 Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in Table 2B row 2. ***Table 2B row 2 Encryption and Decryption of Electronic Health Information for Exchange:*** An encrypted and integrity protected link must be implemented (e.g., TLS, IPv6, IPv4 with IPsec).	There are multiple ways you might demonstrate compliance with this step, including: 1. Identify the encryption method and the tools used for standards based encryption to ensure that the confidentiality of the PHI being transmitted is protected. 2. Identify the protected link (e.g., TLS, IPv6, IPv4 with IPsec) used. 3. Demonstrate the menus, functions, options and the choice for selecting or implementing the methods identified above.

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.06	Demonstrate and describe how the technology provides the capability to 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.	The capability is demonstrated.	IFR.06 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. ***Table 2B row 3 Record Actions Related to Electronic Health Information (i.e., audit log):*** The date, time, patient identification (name or number), and user identification (name or number) must be recorded when electronic health information is created, modified, deleted, or printed. An indication of which action(s) occurred must also be recorded (e.g., modification).	There are multiple ways you might demonstrate compliance with this step, including: 1. Describe and demonstrate the capability to detect auditable events 2. Identify the various audit logs being maintained or used (e.g. operating system log, application logs, database logs, infrastructure logs, etc.) 3. display the content of audit records 4. Demonstrate the ability for authorized users to read (readable format) and interpret the information including date and time, user ID/subject ID, event description, system component where the event occurred, and success and failure of the event. 5. Demonstrate the inability of unauthorized users to access the same logs. 6. Describe and demonstrate the ability to maintain consistent time via the use of NTP/SNTP synchronization 7. Describe and demonstrate the protection of audit records (i.e. access only to authorized users/administrators) 8. Demonstrate the ability to provide alerts based on user-defined events.

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.07	Integrity controls (Addressable). Demonstrate and describe how the technology verifies 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.	The capability is demonstrated.	IFR.07 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. ***Table 2B row 4 Verification that Electronic Health Information has not been Altered in Transit:*** A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm used must be SHA- 1 or higher (e.g., Federal Information Processing Standards (FIPS) Publication (PUB) Secure Hash Standard (SHS) FIPS PUB 180-3).	There are multiple ways you might demonstrate compliance with this step, including: 1. Describe and demonstrate the capability to use checksums 2. Describe and demonstrate the capability to use hashing 3. Describe and demonstrate the capability to detect and create audit trail 4. Describe the technical security measures employed to guard against unauthorized access to the PHI being transmitted 5. Identify the secure transmission method used (e.g., VPN, open protocols such as SSL and TLS) 6. Identify the hashing method and the tools used for standards based hashing (e.g. SHA1, SHA2) to ensure that the transaction has not been tampered in transit 7. Identify the encryption method and the tools used for standards based encryption (e.g. 3DES, AES) to ensure that the confidentiality of the PHI being transmitted is protected. 8. Demonstrate the menus, functions, options and the choice for selecting or implementing the methods identified above

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.08	Person or entity authentication: Demonstrate and describe how the technology verifies that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.	The capability is demonstrated.	IFR.08 Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.	1. There are multiple ways you might demonstrate compliance with this step, including: 2. Identify all services, connections and protocols used for the purposes such as physician's remote access, access using a wireless network, connections used for lab test and diagnostic orders, connections to knowledge-bases, exchanging billing information etc. 3. Describe and demonstrate how remote node authentication is done and what open protocol is used for each service. 4. The ability to provide access only to authenticated users 5. The authentication procedure (e.g. account creation including user IDs, assignment of privileges, 6. The access control method, user-based, RBAC, SSO, EUA, SAML, context-based, etc. 7. The product's password strength rule and password security (age, reuse, display, encryption, etc.) 8. The product's limit of number of consecutive invalid attempt 9. The product's Account lockout after exceeding the limit of number of invalid attempt: - configurable time delay until next login attempt - require release by administrator 10. The ability to suspend user accounts 11. The history of inactive accounts 12. The ability to configure and display notice of warning against unauthorized use 13. The ability to track user IDs in audit records 14. The ability to generate audit records for valid logins and invalid login attempts with user IDs 15.

Procedure		Expected Result	Criteria and Reference	Applicant/Juror Guidance
FND.09	Demonstrate and describe how the technology verifies 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.	The capability is demonstrated.	IFR.09 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. ***Table 2B row 5 Cross-Enterprise Authentication:*** Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (e.g., IHE Cross Enterprise User Assertion (XUA) with SAML identity assertions).	1. Describe and demonstrate the method used for cross-enterprise authentication 2. Describe and demonstrate the capability to authenticate a person or entity across networks 3. Show the account creation and the directory being used. 4. Describe and demonstrate how the identity information is transmitted securely and processed to authenticate persons and entities.

Procedure		**Expected Result**	**Criteria and Reference**	**Applicant/Juror Guidance**
FND.10	Demonstrate and describe how the technology record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in Table 2B row 6.	The capability is demonstrated.	IFR.10 Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in Table 2B row 6. ***Table 2B row 6 Record Treatment, Payment, and Health Care Operations Disclosures:*** The date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded.	The applicant must 1. Describe the method used to record requests for information and the method used to record the disclosures referred to in IFR.10 2. Demonstrate the menus, options and functions via screen displays. 3. Demonstrate the content of the record of disclosure which includes the date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded