Certification Commission
for Health Information
Technology

Test Scripts
For Preliminary ARRA IFR Stage 1 Certification
EHR Technology Security

April 7th, 2010

Product (NUMBER CODE ONLY):_____

Date: _____

Evaluator: _____

Signature: _____

FOUNDATIONAL INFRASTRUCTURE: Security and Privacy

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	Actual Result	Pass/Fail		Criteria and Reference	Comments
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.		❑ Pass	❑ Fail	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.	
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.		❑ Pass	❑ Fail	IFR .02 Permit authorized users (who are authorized for emergency situations) to access electronic health information during an 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.		❑ Pass	❑ Fail	IFR.03 Terminate an electronic session after a predetermined time of inactivity.	

Procedure		Expected Result	Actual Result	Pass/Fail		Criteria and Reference	Comments
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.		❑ Pass	❑ Fail	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).	
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.		❑ Pass	❑ Fail	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).	

Procedure		Expected Result	Actual Result	Pass/Fail		Criteria and Reference	Comments
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.		❑ Pass	❑ Fail	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).	
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.		❑ Pass	❑ Fail	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).	

Procedure		Expected Result	Actual Result	Pass/Fail		Criteria and Reference	Comments
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.		❑ Pass	❑ Fail	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.	
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.		❑ Pass	❑ Fail	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).	
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.		❑ Pass	❑ Fail	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.	