Recommended Standards for Privacy and Security Applicable to 2011 Certification Criteria and Meaningful Use

HIT Standards Committee Source Documents Used in Creating this Matrix Posted at www.healthit.hhs.gov under the HIT Standards Commmittee Link

Services Supported and Functionality Being Addressed	2011 Recommended Underlying Standard	2011 Recommended Implementation Guidance	2011 Recommended Certification Criteria
INFRASTRUCTURE SERVICES			
Consistent Time	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	HITSP/T16 -- Consistent Time	Provide the capability to use NTP to enable a Time Server to provide time to a Time Client.
	IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	HITSP/T16 -- Consistent Time	Provide the capability for Time Clients that are not grouped with a Time Server to use SNTP to obtain time.
	IHE ITI-TF Revision 4.0 or later, Consistent Time (CT) Integration Profile	HITSP/T16 -- Consistent Time	Provide the capability to synchronize the time base between multiple actors and computers using the mechanisms described in the IHE CT profile.
Document Exchange	HITSP/SC112 - Healthcare Document Management	HITSP/SC112 - Healthcare Document Management	Provide the capability to share healthcare documents using a set of topologies, such as Media, e-Mail, Point-to-Point, Shared within a Health Information Exchange, and Shared within a larger community (made up of potentially diverse Health Information Exchanges).
Service Access	OASIS Simple Object Access Protocol (SOAP) Version 1.2	IHE ITI-TF Vol 2: Appendix V (Web Services for IHE Transactions)	For implementations of integration profiles that allow for the use of either SOAP or REST, either SOAP or REST may be used, consistent with the implementation guidance provided by the relevant integration profile.
	OASIS Web Services Security:SOAP Message Security 1.1 (WS-Security 2004), 1 February 2006	IHE ITI-TF Vol 2: Appendix V (Web Services for IHE Transactions)	If SOAP is used to access web services, implement WS-Security security services.
	REST (Representational State Transfer) Note: REST is not a Standards Specification but rather an IT Architectural Style that specifies a series of architecture constraints		
Domain Name Service	IETF: RFC-2181, -2219, -2782. Domain Name Service (DNS) services	HITSP/T64 -- Personnel White Pages	Provide the capability to resolve Internet domain names using DNS.
Directory Access	IETF: RFC-2251, -2252, -2253. Lightweight Directory Access Protocol (LDAP)	HITSP/T64 -- Personnel White Pages -- any directory schema is allowed	Provide the capability to perform intra-enterprise and cross-enterprise directory look-up functions using LDAP
PRODUCT SERVICES			
Access Control	HIPAA	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(a) Access Control (HIPAA)	· Provide capability to allow access only to those persons or software programs that have been granted access rights. · Provide capability to assign a unique name and/or number for identifying and tracking user identity. · Provide capability to access necessary electronic protected health information during an emergency. · Provide capability to terminate an electronic session after a predetermined time of inactivity. · Provide the capability to encrypt and decrypt electronic protected health information.
	FIPS 197, Advanced Encryption Standard, Nov 2001	NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices	Provide the capability to encrypt data at rest using AES.
Audit	HIPAA	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(b) Audit Controls (HIPAA)	Provide the capability to record and examine activity in information systems that contain or use electronic protected health information.
	IHE ITI-TF Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	HITSP/SC109 -- Security Audit	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.
Authentication	HIPAA	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Person or Entity Authentication (HIPAA)	(a) 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. (b) · Provide an authentication mechanism that requires the claimant to prove through a secure authentication protocol that he or she controls the token (e.g., password, private key) presented, and that protects against online guessing, replay, session hijacking, and eavesdropping attacks. · If the authentication mechanism is designed to use long-term shared authentication secrets, implement such that the system never reveals these secrets to any party except the claimant and verifiers that are operated by the credential service provider. · If the system communicates authentication results to third parties (i.e., shares assertions), implement the capability such that all assertions and assertion references are protected from fabrication, modification and reuse attacks, and resistant to disclosure, redirection, capture, and substitution attacks.
Consent Management	HIPAA	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002; American Recovery and Reinvestment Act of 2009 (ARRA), Subtitle D - Privacy. January 6, 2009 (HIPAA)	Provide the capability to electronically record individual consumers' consents and authorizations.
Consumer EHR	HIPAA	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002; American Recovery and Reinvestment Act of 2009 (ARRA), Subtitle D - Privacy. January 6, 2009 (HIPAA)	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.
	HITSP/CAP120 Communicate Unstructured Document (using portable media or system-to-system (PHR) topology)	HITSP/CAP120 Communicate Unstructured Document (using portable media or system-to-system (PHR) topology)	Provide the capability to create and distribute an electronic copy of an individual's EHR as an unstructured document.
De-Identification	HIPAA	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002. Section 164.514(a-b) Deidentification of protected health information (HIPAA)	Provide the capability to remove the identifiers enumerated in Section 164.514(b)(2)(i) of the HIPAA Privacy Rule.
		46 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002. Section 164.514(c) Reidentification (HIPAA)	· 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. · Provide the capability to protect the code or other means of record identification from unauthorized disclosure. provided that:
	ISO/TS 25237:2008 Health Informatics -- Pseudonymisation, Unpublished Technical Specification (Pseudonymization)	HITSP/T24 -- Pseudonymize HITSP/C87 - Anonymize Public Health Case Reporting Data Component HITSP/C88 - Anonymize Immunizations and Response Mgmt Data	Use ISO/TS 25237 as guidance in the implementation of pseudonymization capabilities.
Data Integrity	HIPAA	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(c) Integrity (HIPAA) HITSP/SC112 -- Healthcare Document Management	· Provide the capability to protect electronic protected health information from improper alteration or destruction. · Provide electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
	FIPS PUB 180-3 Secure Hash Standard (SHS). October 2008	FIPS PUB 180-3 Secure Hash Standard (SHS). October 2008	Provide the capability to use one of hash functions in the SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512) to protect the integrity of data at rest.
	ASTM Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	ASTM Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Use as guidance in the design and implementation of electronic signatures.
Transmission Security	HIPAA	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Transmission Security (HIPAA)	· Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. · Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. · Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
	FIPS PUB 180-3 Secure Hash Standard (SHS). October 2008	FIPS PUB 180-3 Secure Hash Standard (SHS). October 2008	Provide the capability to use a secure hash function to protect the integrity of data transmissions. For 2011 certification, the use of SHA-1 is deemed acceptable for generating the message authentication codes (HMACs) used in the TLS protocol; however, use of SHA-1 is not encouraged, and product vendors are encouraged to implement TLS using SHA-224, SHA-256, SHA-384, or SHA-512.
	FIPS 197, Advanced Encryption Standard, Nov 2001	FIPS 197, Advanced Encryption Standard, Nov 2001	Provide the capability to use AES to encrypt data for transmission.
	IETF Transport Layer Security (TLS) Protocol: RFC 2246, RFC 3546	IETF Transport Layer Security (TLS) Protocol: RFC 2246, RFC 3546	Provide the capability to use TLS, with SHA and AES, to establish a mutually authenticated, encrypted, and integrity-protected channel for data exchanges over the World Wide Web. For 2011 certification, the use of SHA-1 is deemed acceptable for generating the message authentication codes (HMACs) used in the TLS protocol; however, use of SHA-1 is not encouraged, and product vendors are encouraged to implement TLS using SHA-224, SHA-256, SHA-384, or SHA-512.