

October 2009 - Certification Standards Recommendations : PRODUCT CERTIFICATION STANDARDS					
Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	<a href="#">Standards Definition</a>	<a href="#">Implementation Timeline note</a>			
Access Control	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(a) Access Control (HIPAA)	HIPAA + AES	HIPAA + AES + HL7 RBAC + SAML + WS-Trust	HIPAA + AES + HL7 RBAC + XACML + SAML + WS-Trust	<ul style="list-style-type: none"> <li>• Provide capability to allow access only to those persons or software programs that have been granted access rights.</li> <li>• Provide capability to assign a unique name and/or number for identifying and tracking user identity.</li> <li>• Provide capability to access necessary electronic protected health information during an emergency.</li> <li>• Provide capability to terminate an electronic session after a predetermined time of inactivity.</li> <li>• Provide the capability to encrypt and decrypt electronic</li> </ul>
	FIPS 197, Advanced Encryption Standard, Nov 2001				Provide the capability to encrypt data at rest using AES.
	HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008				Provide the capability to represent role-based permissions as {operation,object} pairs, using the HL7 permission vocabulary.
	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005				Provide the capability to use XACML access-control policy language and processing model to record and exchange access control information between security domains.
	OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141				Provide the capability exchange user authentication and authorization information between security domains, <u>using the SAML framework.</u>
	OASIS WS-Trust Version 1.3, March 2007				Provide the capability to request and issue security tokens, and to broker trust relationships using WS-Trust.
Audit	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(b) Audit Controls (HIPAA)	HIPAA + ATNA	HIPAA + ATNA	HIPAA + ATNA	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				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	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)	HIPAA(a)	HIPAA(a) + HIPAA(b) + XUA	HIPAA(a) + HIPAA(b) + XUA	(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
	IHE ITI-TF Volume 2 Supplement 2007 – 2008 Cross Enterprise User Assertion (XUA)				(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. Provide the capability to communicate claims about an identity of an authenticated principal (e.g., user, application, system) in transactions that cross enterprise boundaries, as defined in the XUA profile
Consent Management	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)	HIPAA	HIPAA + (CAP143 or BPPC)	HIPAA + (CAP143 or BPPC) + HL7 PrivacyCodes	Provide the capability to electronically record individual consumers' consents and authorizations.
	HITSP/CAP143 Manage Consumer Preference and Consents				Provide the capability to capture and manage consumer consents and authorizations as CDA documents, as described in CAP143.
	IHE ITI-TF Revision 5.0, Basic Patient Privacy Consents (BPPC) Profile				Provide the capability to record consumers' privacy consents and authorizations; to tag documents published to XDS with the privacy consent that was used to authorize the publication; and to enforce the privacy consent appropriate to each use.
	HL7 Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent				Provide the capability to record consumer consents and authorizations using HL7 V3 privacy consent codes.

Consumer EHR	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)	HIPAA + CAP120	HIPAA + CAP119	HIPAA + CAP119	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)				Provide the capability to create and distribute an electronic copy of an individual's EHR as an unstructured document.
	HITSP/CAP119 Communicate Structured 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 a structured Continuity of Care Document (CCD).
HIPAA Deidentification	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)	HIPAA De-identification + HIPAA Re-identification + ISO Pseudonymization	HIPAA De-identification + HIPAA Re-identification + ISO Pseudonymization + HL7 V3 Pedigree	HIPAA De-identification + HIPAA Re-identification + HL7 V3 Pedigree + ISO Pseudonymization	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)				<ul style="list-style-type: none"> <li>• 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.</li> <li>• Provide the capability to protect the code or other means of record identification from unauthorized disclosure.</li> </ul>
	HL7 Version 3.0 Clinical Genomics; Pedigree, Release 1 (Anonymization)				provided that: If the system is capable of persisting and exchanging genomic data, provide the capability to anonymize genomic data using the Pedigree approach.
	ISO/TS 25237:2008 Health Informatics -- Pseudonymisation, Unpublished Technical Specification (Pseudonymization)				Use ISO/TS 25237 as guidance in the implementation of pseudonymization capabilities.
Data Integrity	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(c) Integrity (HIPAA)	HIPAA + SHA + ASTM-Auth	HIPAA + SHA + ASTM-Auth	HIPAA + SHA + ASTM-Auth + (DSG + XadES + TS-17090)	<ul style="list-style-type: none"> <li>• Provide the capability to protect electronic protected health information from improper alteration or destruction.</li> <li>• Provide electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</li> </ul>

	<p>FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1).</p> <p>ASTM Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)</p> <p>HIE ITI-TF Supplement Volume 3 – Document Digital Signature (DSG) Content Profile</p> <p>ETSI Technical Specification TS 101 903: XML Advanced Electronic Signatures (XAdES)</p> <p>ISO/TS-17090, Health Informatics, Public Key Infrastructure</p>				<p>Provide the capability to use SHA to protect the integrity of data at rest.</p> <p>Use as guidance in the design and implementation of electronic signatures.</p> <p>Provide the capability to digitally sign documents shared between organizations, using XAdES advanced electronic signatures. Use ISO/TS-17090 as guidance in implementing the use of digital certificates to digitally sign electronic documents using DSG.</p>
Transmission Security	<p>45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Transmission Security (HIPAA)</p>	HIPAA + SHA-2 + AES + TLS	HIPAA + SHA-2 + AES + TLS	HIPAA + SHA-2 + AES + TLS + CMS	<ul style="list-style-type: none"> <li>• Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</li> <li>• Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.</li> <li>• Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.</li> </ul>
	<p>FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1).</p> <p>FIPS 197, Advanced Encryption Standard, Nov 2001</p> <p>IETF Transport Layer Security (TLS) Protocol: RFC 2246, RFC 3546</p> <p>IETF Cryptographic Message Syntax (CMS), RFC-2630, -3852</p>				<p>Provide the capability to use SHA to protect the integrity of data transmissions.</p> <p>Provide the capability to use AES to encrypt data for transmission.</p> <p>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 <u>World Wide Web</u></p> <p>If an email capability is provided, implement the CMS standard to cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption.</p>








---

Standards Definition: Includes regulatory standards, standards developed by Standards Development Organizations (SDOs), and standards developed by Profile-Enforcement Organizations (PEOs)  
Implementation Timeline note: Minimal standards for targeted year. Earlier implementation of standards specified for 2013 or 2015 is encouraged.



October 2009 - Standards Implementation Guidance: PRODUCT CERTIFICATION STANDARDS				
Functionality	Standards	Implementation Guidance (2011)	Implementation Guidance (2013-2015)	Gaps, Notes, Comments, and Future
Access Control	45 CFR Parts 160, 162, and 164 Health			
	FIPS 197, Advanced Encryption Standard, Nov 2001	NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices		
	HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008		HITSP/SC108 -- Access Control (Using any implementation of RBAC that supports permissions from the HL7 permissions catalog)	
	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005		HITSP/SC108 -- Access Control (exchanging privacy policy in computable form using healthcare specific XACML schema)	Contingent on availability of healthcare specific XML schema, user attributes, role codes, etc.
	OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141		HITSP/SC108 -- Access Control (Using C19/SAML assertions supporting healthcare specific attribute schema)	Contingent on availability of healthcare specific XML schema, user attributes, role codes, etc.
	OASIS WS-Trust Version 1.3, March 2007		HITSP/SC108 -- Access Control (Supporting federated identity domains through use of WS-Trust channel between identity providers)	Contingent on availability of healthcare specific XML schema, user attributes, role codes, etc.
Audit	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(b) Audit Controls (HIPAA)			
	IHE ITI-TF Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	HITSP/SC109 -- Security Audit		
Authentication	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)		NIST SP 800-63-1 - Electronic Authentication Guideline	

	IHE ITI-TF Volume 2 Supplement 2007 – 2008 Cross Enterprise User Assertion (XUA)		HITSP/C19 -- Entity Identity Assertion	
Consent Management	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)			Standards work continues that will support more expressive policies than can be acknowledged today
	HITSP/CAP143 Manage Consumer Preference and Consents		HITSP/CAP143 -- Manage Consumer Preferences and Consents	
	IHE ITI-TF Revision 5.0, Basic Patient Privacy Consents (BPPC) Profile		HITSP/CAP143 -- Manage Consumer Preferences and Consents	
	HL7 Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent		HITSP/CAP143 -- Manage Consumer Preferences and Consents	
Consumer EHR	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)			
	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)		
	HITSP/CAP119 Communicate Structured Document (using portable media or system-to-system (PHR) topology)		HITSP/CAP119 Communicate Structured Document (using portable media or system-to-system (PHR) topology)	
HIPAA Deidentification	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)			

	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)			
	HL7 Version 3.0 Clinical Genomics; Pedigree, Release 1 (Anonymization)		HITSP/C25 - Anonymize (for Biosurveillance and Quality)	
	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		
Data Integrity	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		Data Integrity is provided for low/moderate level of assurance through SHA1 hash/size independently managed from the document
	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1)		HITSP/C26 -- Nonrepudiation of Origin	
	ASTM Standard Guide for Electronic Authentication of Health Care Information: # F1762-95(2003)		HITSP/C26 -- Nonrepudiation of Origin	
	HIE ITI-TF Supplement Volume 3 – Document Digital Signature (DSG) Content Profile		HITSP/C26 -- Nonrepudiation of Origin	
	ETSI Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)		HITSP/C26 -- Nonrepudiation of Origin	
	ISO/TS-17090, Health Informatics, Public Key Infrastructure		HITSP/C26 -- Nonrepudiation of Origin	
Transmission Security	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Transmission Security (HIPAA)			



October 2009 - Standards Implementation Guidance: INFRASTRUCTURE CERTIFICATION STANDARDS				
Functionality	Standards	Implementation Guidance (2011)	Implementation Guidance (2013-2015)	Gaps, Notes, Comments, and Future
Consistent Time	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	HITSP/T16 -- Consistent Time		
	IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	HITSP/T16 -- Consistent Time		
	IHE ITI-TF Revision 4.0 or later, Consistent Time (CT) Integration Profile	HITSP/T16 -- Consistent Time		
Document Exchange	HITSP/SC112 - Healthcare Document Management	HITSP/SC112 -- Healthcare Document Management		
	IHE ITI-TF Cross Enterprise Document Reliable Interchange (XDR) Integration Profile		HITSP/SC112 -- Healthcare Document Management	
	IHE ITI-TF Revision 5.0 Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b) Integration Profile		HITSP/SC112 -- Healthcare Document Management	
	IHE ITI-TF Revision 5.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]		HITSP/SC112 -- Healthcare Document Management	
	OASIS/ebXML Registry Information Model v3.0		HITSP/SC112 -- Healthcare Document Management	
	OASIS/ebXML Registry Services (ebRS) Specifications v3.0		HITSP/SC112 -- Healthcare Document Management	
	IHE ITI-TF Revision 5.0 or later, Cross Community Access (XCA) profile		HITSP/SC112 -- Healthcare Document Management	
	IHE ITI-TF Revision 5.0 or later, Cross-Enterprise Document Media Interchange (XDM) Integration Profile		HITSP/SC112 -- Healthcare Document Management	
	HL7 V3 Confidentiality Codes value set		HITSP/SC112 -- Healthcare Document Management	
Service Access	OASIS Simple Object Access Protocol (SOAP) Version 1.2	IHE ITI-TF Vol 2: Appendix V (Web Services for IHE Transactions)		
	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)		
Domain Name Service	IETF: RFC-2181, -2219, -2782. Domain Name Service (DNS) services	HITSP/T64 -- Personnel White Pages		
Directory Access	IETF: RFC-2251, -2252, -2253. Lightweight Directory Access Protocol (LDAP)	HITSP/T64 -- Personnel White Pages -- any directory schema is allowed		HITSP is working on a cross-enterprise provider directory

	IHE ITI-TF Revision 4.0 or later, Personnel White Pages (PWP)		HITSP/T64 -- Personnel White Pages -- conformant directory schema required	
	RFC 1766 Tags for the Identification of Languages		HITSP/T64 -- Personnel White Pages	