

## PRIVACY AND SECURITY STANDARDS APPLICABLE TO ARRA REQUIREMENTS (August 20, 2009 Update)

Source Refs/ Cross-Refs	Standard	Services Supported	Recommended Implementation Timeframe		
			2011	2013	2015
HITSP TP20/SC108	HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008 [1]	Access control		x	
HITSP TP20/SC108	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	Access control			x
HITSP C19/TP20/SC108	OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141 [2]	Access control		x	
HITSP TP20/SC108	OASIS WS-Trust Version 1.3, March 2007	Access control		x	
HITSP T15/T17/SC109	IHE ITI-TF Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	Audit		x	
<i>IHE EUA</i>	IETF RFC 4120. The Kerberos Network Authentication Service (V5). July 2005	Authentication	x		
HITSP TP30	IHE ITI-TF Revision 5.0 Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	Authentication; Consent management		x	
	IHE ITI-TF Revision 5.0 or later, Enterprise User Authentication (EUA) profile	Authentication	x		
HITSP C19	IHE ITI-TF Volume 2 Supplement 2007 – 2008 Cross Enterprise User Assertion (XUA) [3]	Authentication		x	
HITSP C19; <i>IHE Registry Query; IHE XDS.b</i>	OASIS Simple Object Access Protocol (SOAP) Version 1.1 [4]	Authentication	x		

HITSP CAP143	HITSP/CAP143 Manage Consumer Preference and Consents	Consent management		x	
HITSP TP30	HL7 Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent [1]	Consent management			x
HITSP TP30	IHE ITI-TF Revision 5.0, Basic Patient Privacy Consents (BPPC) Profile [5]	Consent management		x	
HITSP TP30	IHE ITI-TF Revision 5.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	Consent management			
<i>IHE Registry Query</i>	OASIS/ebXML Registry Information Model v3.0	Consent management		x	
<i>IHE Registry Query</i>	OASIS/ebXML Registry Services (ebRS) Specifications v3.0	Consent management		x	
HITSP T16; <i>IHE Consistent Time</i>	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	Consistent time	x		
HITSP T16; <i>IHE Consistent Time</i>	IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	Consistent time	x		
HITSP T16; <i>IHE Consistent Time</i>	IHE ITI-TF Revision 4.0 or later, Consistent Time (CT) Integration Profile [6]	Consistent time	x		
HITSP CAP119	Communicate Structured Document (using portable media or system-to-system (PHR) topology)	Consumer EHR		x	
HITSP CAP120	Communicate Unstructured Document (using portable media or system-to-system (PHR) topology)	Consumer EHR	x		
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. (Deidentification)	Deidentification	x		
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 (Pseudonymization)	Deidentification	x		

HITSP T24/C25/C88	ISO/TS 25237:2008 Health Informatics -- Pseudonymisation, Unpublished Technical Specification (Pseudonymization) [7]	Deidentification			x
HITSP C87	HL7 Version 3.0 Clinical Genomics; Pedigree, Release 1 (Anonymization) [1]	Deidentification		x	
<i>IHE PWP</i>	IETF: RFC-2181, -2219, -2782 (DNS services)	Identity Management	x		
<i>IHE PWP</i>	IETF: RFC-2251, -2252, -2253 (LDAP)	Identity Management	x		
HITSP T64	IHE ITI-TF Revision 4.0 or later, Personnel White Pages (PWP)	Identity Management		x	
HITSP C19	OASIS Web Services Security:SOAP Message Security 1.1 (WS-Security 2004), 1 February 2006 [4]	Identity Management	x		
<i>IHE PWP</i>	RFC 1766 Tags for the Identification of Languages	Identity Management	x		
HITSP TP30	IHE ITI-TF Revision 5.0 or later, Cross Community Access (XCA) profile	Infrastructure		x	
HITSP C26	ETSI Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	Non-repudiation			x
HITSP C26	ASTM Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Non-Repudiation	x		
HITSP C26	HIE ITI-TF Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Non-repudiation			x
<i>IHE XDM</i>	IETF Cryptographic Message Syntax, RFC-2630, -3852	Non-repudiation; secure email	x		
<i>IHE DSG</i>	ISO/TS-17090, Health Informatics, Public Key Infrastructure	Non-repudiation			x
<i>IHE ATNA</i>	FIPS 197, Advanced Encryption Standard, Nov 2001	Secure transmission	x		
<i>IHE ATNA</i>	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1).	Secure transmission	x		
<i>IHE ATNA</i>	IETF Transport Layer Security (TLS) Protocol: RFC 2246, RFC 3546 [8]	Secure transmission	x		
<i>IHE BPPC</i>	IHE ITI-TF Cross Enterprise Document Reliable Interchange (XDR)	Secure transmission		x	
HITSP T33	IHE ITI-TF Revision 5.0 or later, Cross-Enterprise Document Media Interchange (XDM) Integration Profile [9]	Secure email		x	

NOTES:

- [1] HL7 V3 constructs are gaining traction in the marketplace.
- [2] SAML is a well established standard set, with broad support from security vendors, but cannot be considered fully accepted. Also, with respect to healthcare use, SAML lacks a standardized set of attributes and vocabulary to enable its use between enterprises (e.g., HIEs).
- [3] XUA uses a subset of SAML for inter-enterprise exchanges -- therefore rated 2, consistent with inter-enterprise SAML.
- [4] SOAP is generally specified for web-services (WS) messaging in IHE profiles and HITSP constructs, so the SOAP standard and WS standards referenced by the HITSP constructs are included here. However, recent technology trends in web development are showing REpresentational State Transfer (REST) emerging as an alternative solution for eliminating some of the complexity associated with the WS-\* standards. REST is not a new standard; rather it uses the "HTTP GET" command with a URI to retrieve the desired content. IHE ATNA (HITSP T17) accommodates both WS-\* and REST. So rather than recommending one over the other, the Privacy and Security WG is recommending that both REST and SOAP be recognized as acceptable web-development design approaches.
- [5] Really just a special case of XDS, BPPC stores and retrieves to/from a document repository a document containing an individual's consents. It does not interpret those consents nor integrate them with access control.
- [6] Uses NTP and SNTP, both of which are quite mature.
- [7] Discusses pseudonymization, but is not a technical specification.
- [8] Requires integrity protection -- i.e., no NULL\_NULL
- [9] Addresses sending of sensitive documents (ZIP files) over email secured using S/MIME (also used in IHE ATNA).