

HIT Standards Committee

**Privacy and Security Workgroup:
Reformatted Standards Recommendations
& Implementation Guidance**

Dixie Baker, SAIC

Steven Findlay, Consumers Union

September 15, 2009

Privacy and Security Workgroup Members

- Dixie Baker, SAIC
- Anne Castro, BlueCross BlueShield of South Carolina
- Aneesh Chopra, Federal Chief Technology Officer
- David McCallie, Cerner Corporation
- John Moehrke, HITSP
- Steve Findley, Consumers Union
- Gina Perez, Delaware Health Information Network
- Sharon Terry, Genetic Alliance
- Wes Rishel, Gartner
- John Moehrke, HITSP
- Ed Larsen, HITSP

Tasks from August 2009 Standards Committee Meeting

1. Reformat certification standards recommendations to:
 - Incorporate the technical requirements from the HIPAA Security and Privacy Rules (plus ARRA) that comprise the baseline (2011) requirements for product certification
 - Clarify where options exist – that is, standards that are required jointly (e.g., standard A + standard B) and standards for which the implementer is given a choice (e.g., standard A or standard B)
 - Include high-level certification criteria statements
2. Identify and recommend implementation guidance documents to help system developers and integrators implement the recommended standards

Work Products Presented to the Committee Today

- Handout #1 Reformatted Standards, Timeline, and Certification Criteria
 - Requirements for certifying that products provide the capabilities required to support HIPAA/ARRA security and privacy requirements and best practices for “meaningful use”
 - Update submitted for approval by the full Committee
- Handout #2 Implementation guidelines for recommended standards
 - Submitted for approval by the full Committee

Reformatted Standards – Handout #1

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	Includes regulatory standards, standards developed by Standards Development Organizations (SDOs), and standards developed by Profile-Enforcement Organizations (PEOs)	Minimal standards for targeted year. Earlier implementation of standards specified for 2013 or 2015 is encouraged.			
PRODUCT CERTIFICATION STANDARDS					
Access Control	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2013. 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"> 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.
	Standard, ITU-T X.1141				Provide the capability to encrypt data at rest using AES.
	Version 1.3, March 2009				Provide the capability to represent role-based permissions as (operation,object) pairs, using the HL7 permission vocabulary.
					Provide the capability to use XACML access-control policy language and processing model to record and exchange access control information between security domains.
					Provide the capability exchange user authentication and authorization information between security domains, using the SAML framework.
					Provide the capability to exchange user authentication and authorization information between security domains, using the SAML framework.
					Provide the capability to exchange user authentication and authorization information between security domains, using the SAML framework.
					cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption.
INFRASTRUCTURE CERTIFICATION STANDARDS					
Consistent Time	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	CT + (NTP or SNTP)	CT + (NTP or SNTP)	CT + (NTP or SNTP)	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				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				Provide the capability to synchronize the time base between multiple actors and computers using the mechanisms described in the IHE CT profile.

Includes regulatory standards, standards developed by Standards Development Organizations (SDOs), and standards developed by Profile-Enforcement Organizations (PEOs).

Reformatted Standards – Handout #1

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	Includes regulatory standards, standards developed by Standards Development Organizations (SDOs), and standards developed by Profile-Enforcement Organizations (PEOs)	Minimal standards for targeted year. Earlier implementation of standards specified for 2013 or 2015 is encouraged.			
PRODUCT CERTIFICATION STANDARDS					
Access Control	<p>45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(a) Access Control (HIPAA)</p> <p>FIPS 197, Advanced Encryption Standard, Nov 2001</p> <p>HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008</p> <p>OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005</p> <p>OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141</p> <p>Version 1.3, March 2003</p>	HIPAA + AES	HIPAA + AES + HL7 RBAC + SAML + WS-Trust	HIPAA + AES + HL7 RBAC + XACML + SAML + WS-Trust	<ul style="list-style-type: none"> 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. <p>Provide the capability to encrypt data at rest using AES.</p> <p>Provide the capability to represent role-based permissions as (operation,object) pairs, using the HL7 permission vocabulary.</p> <p>Provide the capability to use XACML access-control policy language and processing model to record and exchange access control information between security domains.</p> <p>Provide the capability exchange user authentication and authorization information between security domains, using the SAML framework.</p> <p>Provide the capability to...</p>
					cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption.
INFRASTRUCTURE CERTIFICATION STANDARDS					
Consistent Time	<p>IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992</p> <p>IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996</p> <p>IHE ITI-TF Revision 4.0 or later, Consistent Time (CT) Integration Profile</p>	CT + (NTP or SNTP)	CT + (NTP or SNTP)	CT + (NTP or SNTP)	<p>Provide the capability to use NTP to enable a Time Server to provide time to a Time Client.</p> <p>Provide the capability for Time Clients that are not grouped with a Time Server to use SNTP to obtain time.</p> <p>Provide the capability to synchronize the time base between multiple actors and computers using the mechanisms described in the IHE CT profile.</p>

Reformatted Standards – Handout #1

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	Includes regulatory standards, standards developed by Standards Development Organizations (SDOs), and standards developed by Profile-Enforcement Organizations (PEOs)	Minimal standards for targeted year. Earlier implementation of standards specified for 2013 or 2015 is encouraged.			
PRODUCT CERTIFICATION STANDARDS					
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 + WS-Trust	Provide capability to allow access only to those persons or programs that have been granted access rights. Provide the capability to assign a unique name and/or number for tracking user identity.
	FIPS 197, Advanced Encryption Standard, Nov 2001				
	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, using the SAML framework.
	...				Provide the ... and to
					cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption.
INFRASTRUCTURE CERTIFICATION STANDARDS					
Consistent Time	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	CT + (NTP or SNTP)	CT + (NTP or SNTP)	CT + (NTP or SNTP)	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				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				Provide the capability to synchronize the time base between multiple actors and computers using the mechanisms described in the IHE CT profile.

Minimal standards for targeted year. Earlier implementation of standards specified for 2013 or 2015 is encouraged.

Reformatted Standards – Handout #1

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	Includes regulatory standards, standards developed by Standards Development Organizations (SDOs), and standards developed by Profile-Enforcement Organizations (PEOs)	Minimal standards for targeted year. Earlier implementation of standards specified for 2013 or 2015 is encouraged.			

Product Certification Standards (derived from HIPAA Privacy and Security Rules)

	Standards: Final Rule: February 20, 2005: § 104.312(a) Access Control (HIPAA)		HL7 RBAC + SAML + WS-Trust	HL7 RBAC + XACML + SAML + WS-Trust	<p>software programs that have been granted access rights.</p> <ul style="list-style-type: none"> 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				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, using the SAML framework.
	Version 1.3, March 2003				Provide the capability to exchange user authentication and authorization information between security domains, and to

cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption.

Infrastructure Certification Standards (needed to support meaningful use)

	Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	SNTP	SNTP	SNTP	time to a Time Client.
	IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996				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				Provide the capability to synchronize the time base between multiple actors and computers using the mechanisms described in the IHE CT profile.

Notable Changes

Change	Justification
IHE ATNA required for 2011	ARRA requirement for accounting of disclosures
Kerberos/EU authentication allowed only in 2011	Pending change in federal policy will prohibit the use of Kerberos for authentication in federal systems
Choice among XDS suite (XDS.b, RegQuery, ebXML RIM, and ebRS); XDR; XCA; and XDM for reliably exchanging electronic health records; Basic SC112 for 2011	Need for clarification among choices for document exchanges; need to add basic document exchange for 2011 (SC112)
Allow (SOAP + WS-Security) or REST for profiles that provide implementation guidance	Need to constrain use of REST

Implementation Guidance Selection

- Recommend clear guidance that is most likely to produce real interoperability between enterprises
- Draw from any of the following documentation sets (from highest to lowest priority):
 1. HITSP Tiger Team products (capabilities, service collaborations)
 2. HITSP use-case-based constructs (Interoperability Specifications, Transaction Packages, Transactions, Components)
 3. IHE Profiles or profiles produced by other profiler-enforcer organizations
 4. Standards published by SDOs

Recommended Implementation Guidance – Handout #2

Functionality	Standards	Implementation Guidance (2011)	Implementation Guidance (2013-2015)	Gaps, Notes, Comments, and Future Enhancements
PRODUCT CERTIFICATION STANDARDS				
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)			
	FIPS 197, Advanced Encryption Standard, Nov 2001	NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices		
	HL7 V3 RBAC, R3-2008; 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)			
	4.0 or later, Audit Trail	HITSP/SC109 -- Security Audit		
	IETF Cryptographic Message Syntax (CMS), RFC-2630, 3852	HITSP/T17 -- Secure Communications		
INFRASTRUCTURE CERTIFICATION STANDARDS				
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		

Recommended Implementation Guidance – Handout #2

Functionality	Standards	Implementation Guidance (2011)	Implementation Guidance (2013-2015)	Gaps, Notes, Comments, and Future Enhancements
PRODUCT CERTIFICATION STANDARDS				
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)			
	FIPS 197, Advanced Encryption Standard, Nov 2001	HITSP/T11 - Guide to Storage Encryption for End User Devices		
	HL7 V3 RBAC, R3-2008; HL7 Version 3 Standard Based Access Control (RBAC) Healthcare		HITSP/SC108 -- Access Control (Using any implementation of RBAC that supports permissions from the HL7 permissions catalog)	
			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.
			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)			
		HITSP/SC109 -- Security Audit		
	IETF Cryptographic Message Syntax (CMS), RFC-2630, 3852	HITSP/T17 -- Secure Communications		
INFRASTRUCTURE CERTIFICATION STANDARDS				
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		

Implementation guidance for those standards required by 2011

Recommended Implementation Guidance – Handout #2

Functionality	Standards	Implementation Guidance (2011)	Implementation Guidance (2013-2015)	Gaps, Notes, Comments, and Future Enhancements
PRODUCT CERTIFICATION STANDARDS				
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)			
	FIPS 197, Advanced Encryption Standard, Nov 2001	NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices		
	HL7 V3 RBAC, R3-2008; 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)			
	4.0 or later, Audit Trail	HITSP/SC109 -- Security Audit		
	IETF Cryptographic Message Syntax (CMS), RFC-2630, 3852	HITSP/T17 -- Secure Communications		
INFRASTRUCTURE CERTIFICATION STANDARDS				
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		

Recommended Implementation Guidance – Handout #2

Functionality	Standards	Implementation Guidance (2011)	Implementation Guidance (2013-2015)	Gaps, Notes, Comments, and Future Enhancements	
PRODUCT CERTIFICATION STANDARDS					
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)				
	FIPS 197, Advanced Encryption Standard, Nov 2001	NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices			
	HL7 V3 RBAC, R3-2008; HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008		HITSP/SC108 -- Access Control (Role-based permissions implementation of RBAC from the HL7 permissions catalog)		
	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005		HITSP/SC108 -- Access Control (Role-based permissions implementation of 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 (Role-based permissions implementation of SAML 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 (Role-based permissions implementation of WS-Trust schema)	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)				

Implementation guidance for those standards required for 2013-2015, and optional for 2011

	IETF Cryptographic Message Syntax (CMS), RFC-2630, 3852	HITSP/T17 -- Secure Communications		
INFRASTRUCTURE CERTIFICATION STANDARDS				
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		

Recommended Implementation Guidance – Handout #2

Functionality	Standards	Implementation Guidance (2011)	Implementation Guidance (2013-2015)	Gaps, Notes, Comments, and Future Enhancements
PRODUCT CERTIFICATION STANDARDS				
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)			
	FIPS 197, Advanced Encryption Standard, Nov 2001	NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices		
	HL7 V3 RBAC, R3-2008; 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)			
	4.0 or later, Audit Trail	HITSP/SC109 -- Security Audit		
	IETF Cryptographic Message Syntax (CMS), RFC-2630, 3852	HITSP/T17 -- Secure Communications		
INFRASTRUCTURE CERTIFICATION STANDARDS				
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		

Selected Guidelines – HITSP Tiger Team Products

- HITSP Capabilities
 - CAP119 – Communicate Structured Document
 - CAP120 – Communicate Unstructured Document
 - CAP143 – Managing Consumer Preferences & Consents
- HITSP Service Collaborations
 - SC108 – Access Control
 - SC109 – Security Audit
 - SC112 – Healthcare Document Management

Selected Guidelines – HITSP Constructs

- HITSP Components
 - C19 – Entity Identity Assertion
 - C25 – Anonymize (for Biosurveillance and Quality)
 - C26 – Nonrepudiation of Origin
 - C87 – Anonymize Public Health Case Reporting Data
 - C88 – Anonymize Immunizations and Response Management Data
- HITSP Transactions
 - T16 – Consistent Time
 - T17 – Secure Communications Channel
 - T24 – Pseudonymize
 - T64 – Personnel White Pages

Selected Guidelines – Other

- IHE
 - EUA Integration Profile
 - ITI-TF Volume 2: Appendix V (Web Services for IHE Transactions)
- NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices