October 2009 - Certification Standards Recommendations: PRODUCT DEFINITIONS		
Functionality	**Standards**	**Basic Definition**
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)	Access Control is the first Technical Safeguard Standard of the HIPAA Administrative Simplification Security Rule. It has four implementation specifications: unique user identification; emergency access procedure; automatic logoff; and encryption and decryption. To comply with the HIPAA Security Rule, an organization is required to implement the first two, and the latter two are addressable. But to get a product certified, a vendor must implement functions to support all implementation specifications. "Addressable" does not mean “optional.” Rather, an addressable implementation specification means that a covered entity must use reasonable and appropriate measures to meet the standard.
	FIPS 197, Advanced Encryption Standard, Nov 2001	Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. AES comprises three block ciphers. Each cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
	HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	Role-based access control (RBAC)is an approach to restricting system access to authorized users. RBAC is sometimes referred to as role-based security. To conform to role-based access control standards, a role definition consists of a name and a corresponding set of permissions as defined in the Health Level 7 (HL7) permission vocabulary. This vocabulary provides access control information supporting access control decision and enforcement functions.
	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	XACML provides a necessary component for complex, interactive Web services, enterprisewide security management and Digital Rights Management (DRM). Using XACML, an enterprise can define platform-independent rules for how its resources are used by those inside and outside the enterprise. Enterprises can work together without having to align their computing platforms (whether based on Java, .NET or another technology); they just have to align their access policies.
	OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141	SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application, as defined in the ITU standard.
	OASIS WS-Trust Version 1.3, March 2007	Web Services Trust Language (WS-Trust) uses the secure messaging mechanisms of WS-Security to define additional extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. In order to secure a communication between two parties, the two parties must exchange security credentials (either directly or indirectly). However, each party needs to determine if they can "trust" the asserted credentials of the other party.

Functionality	Standards	Basic Definition
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 Audit Controls requires the implementation of hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.
	IHE ITI-TF Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	The Audit Trail and Node Authentication (ATNA) Integration Profile establishes security measures which, together with the Security Policy and Procedures, provide patient information confidentiality, data integrity and user accountability
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 Authentication requires the Implementation of procedures to verify that a person or entity seeking access is the one claimed.
	IHE ITI-TF Volume 2 Supplement 2007 – 2008 Cross Enterprise User Assertion (XUA)	The Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries.

Functionality	Standards	Basic Definition
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)	The HIPAA Privacy Rule sets forth standards for requiring and obtaining a consumer's consent for the use of his or her Protected Health Information (PHI).
	HITSP/CAP143 Manage Consumer Preference and Consents	CAP143 addresses management of consumer preferences and consents as an acknowledgement of a privacy policy. This capability is used to capture a patient or consumer agreement to one or more privacy policies; where examples of a privacy policy may represent a consent, dissent, authorization for data use, authorization for organizational access, or authorization for a specific clinical trial. This capability also supports the recording of changes to prior privacy policies such as when a patient changes their level of participation or requests that data no-longer be made available because they have left the region.
	IHE ITI-TF Revision 5.0, Basic Patient Privacy Consents (BPPC) Profile	BPPC, Basic Patient Privacy Consent Includes three key parts: 1. Content module for capturing a patient consent to a privacy policy or policies. 2. Describes how the confidentialityCode attribute of the XDSDocumentEntry metadata is used to support the consent policies. 3. Describes the method by which XDS Consumer Actors can enforce the privacy policies determined by the document confidentialityCode and the patient privacy consents.
	HL7 Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	Privacy Consent references an individual's right to access his or her PHI is a critical aspect of the Privacy Rule, the application of which naturally extends to an electronic environment. The Privacy Rule establishes, with limited exceptions, an enforceable means by which individuals have a right to review or obtain copies of their PHI, to the extent it is maintained in the designated record set(s) of a covered entity. The Privacy Rule's specific, yet flexible, standards also address individuals' requests for access and timely action by the covered entity, including the provision of access, denial of access, and documentation. The Openness and Transparency Principle in the Privacy and Security Framework emphasizes the concept that trust in electronic health information exchange can best be established in an open and transparent environment. It also stresses that it is important for individuals to understand what individually identifiable health information exists about them, how that information is collected, used, and disclosed, and how reasonable choices can be exercised with respect to that information.

Functionality	Standards	Basic Definition
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)	The HIPAA Privacy Rule sets forth standards for providing consumers copies of their Protected Health Information (PHI).
	HITSP/CAP120 Communicate Unstructured Document (using portable media or system-to-system (PHR) topology)	CAP120 addresses interoperability requirements that support the communication of a set of unstructured health data related to a patient in a context set by the source of the document who is attesting to its content.
	HITSP/CAP119 Communicate Structured Document (using portable media or system-to-system (PHR) topology)	CAP119addresses interoperability requirements that support the communication of structured health data related to a patient in a context set by the source of the document who is attesting to its content. Several document content subsets, structured according to the HL7 Clinical Document Architecture standard, are supported by this capability.

Functionality	Standards	Basic Definition
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 Deidentification specifies that de-identified PHI is rendered anonymous when identifying characteristics are completely removed. PHI must be de-identified prior to disclosure to non-authorized users. Specifies data elements that must be removed to render PHI "deidentified."
	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)	HIPAA Reidentification specifies that identifier may be generated to re-identify data. More definition than specification.
	HL7 Version 3.0 Clinical Genomics; Pedigree, Release 1 (Anonymization)	The HL7 Clinical Genomic Pedigree is an XML-based message markup standard that specifies the structure and semantics of family history for the purpose of exchange.
	ISO/TS 25237:2008 Health Informatics -- Pseudonymisation, Unpublished Technical Specification (Pseudonymization)	ISO/TS 25237:2008, Health informatics – Pseudonymization, contains principles and requirements for privacy protection using pseudonymization services for the protection of personal health information in databases. Pseudonymization (from pseudonym) allows for the removal of an association with a data subject. It differs from anonymization (anonymous) in that it allows for data to be linked to the same person across multiple data records or information systems without revealing the identity of the person. The technique is recognized as an important method for privacy protection of personal health information. It can be performed with or without the possibility of re-identifying the subject of the data (reversible or irreversible pseudonymization).

Functionality	Standards	Basic Definition
Data Integrity	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(c) Integrity (HIPAA)	Implement policies and procedures to protect data from improper aleration or destruction.
	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1)	Specifies secure hash functions used by TLS. NIST Policy (March 15, 2006) specifies that the SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms. No use of SHA-1 after 2010.
	ASTM Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Standard on the design, implementation, and use of electronic signatures in health care.
	HIE ITI-TF Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. Regarding digital security, the meaning and application of non-repudiation shifts to mean a service that provides proof of the integrity and origin of data. An authentication that with high assurance can be asserted to be genuine. Proof of data integrity is typically the easiest of these requirements to accomplish. A data hash, such as SHA1, is usually sufficient. A hash function is any well-defined procedure or mathematical function which converts a large, possibly variable-sized amount of data into a small datum (singular form of data).
	ETSI Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	Advanced Electronic Signatures defines Advanced formats for Electronic Signatures in XML syntaxes.
	ISO/TS-17090, Health Informatics, Public Key Infrastructure	Health Informatics, Public Key Infrastructure (ISO/TS-17090) gives guidelines for certificate management issues involved in deploying digital certificates in healthcare. It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements.

Functionality	Standards	Basic Definition
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)	Transmission Security implements technical security measures to guard against un authorized access to data transmitted over a network.
	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1)	SHA, secure hash algorithms specifies secure hash functions used by TLS. NIST Policy (March 15, 2006) specifies that the SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms. No use of SHA-1 after 2010.
	FIPS 197, Advanced Encryption Standard, Nov 2001	Advanced Encryption Standards is an encryption standard adopted by the U.S. government. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. AES comprises three block ciphers. Each cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
	IETF Transport Layer Security (TLS) Protocol: RFC 2246, RFC 3546	Transport Layer Security Provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
	IETF Cryptographic Message Syntax (CMS), RFC-2630, -3852	CMS Cryptographic Message Syntax, is the IETF's standard for cryptographically protecting messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data. Based on the syntax of PKCS#7, which in turn is based on the Privacy-Enhanced Mail standard. The newest version of CMS (as of 2004) is specified in RFC 3852. The architecture of CMS is built around certificate-based key management. CMS is used as the key cryptographic component of many other cryptographic standards, such as S/MIME, PKCS#12 and the RFC 3161 Digital timestamping protocol.

October 2009 - Certification Standards Recommendations: INFRASTRUCTURE DEFINITIONS		
Functionality	**Standards**	**Basic Definition**
Consistent Time	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	Network Time Protocol is a protocol (a set of rules governing the format of messages that are exchanged between computers) for synchronizing the clocks of computer systems over data networks. It is designed particularly to resist the effects of variable latency.
	IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	Simple Network Time Protocol (SNTP) Version 4, is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. It is recommended that you use second-level time servers for normal time server configuration because they are usually located on a closer network that can produce faster updates.
	IHE ITI-TF Revision 4.0 or later, Consistent Time (CT) Integration Profile	Consistent Time Integration Profile provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronized. This profile specifies synchronization with a median error of less than 1 second.

Functionality	Standards	Basic Definition
Document Exchange	HITSP/SC112 - Healthcare Document Management	The HITSP/SC112 Healthcare Document Management provides the ability to share healthcare documents using a set of topologies (methods) 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.
	IHE ITI-TF Cross Enterprise Document Reliable Interchange (XDR) Integration Profile	XDR allows data to be wrapped in an architecture independent manner so data can be transferred between varied computer systems. Converting from the local representation to XDR is called *encoding* . Converting from XDR to the local representation is called *decoding* . XDR is implemented as a software library of functions that is portable between different operating systems and is also independent of the transport layer.
	IHE ITI-TF Revision 5.0 Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b) Integration Profile	Integration Profile XDS.b is a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on a use of the Web Services and ebXML Reg/Rep, a standard under the E-Business XML umbrella which provides an integrated registry and repository that is consistent with the current developments and best practices in the industry.
	IHE ITI-TF Revision 5.0 - Registry Stored Query Transaction for XDS Profile	Cross Enterprise Document Sharing (XDS) is a system defined by IHE for sharing clinical documents between institutions
	OASIS/ebXML Registry Information Model OASIS/ebXML Registry Services (ebRS) Specifications v3.0	OASIS/ebXML Registry Information Model v3.0 is a family of Extensible Markup Language (XML) based standards sponsored by the Organization for the Advancement of Structured Information Standards (OASIS) whose mission is to provide an open, XML-based infrastructure that enables the global use of electronic business information in an interoperable, secure, and consistent manner by all trading partners. XML is a set of rules for encoding (transforming information from one format to another) documents electronically.
	IHE ITI-TF Revision 5.0 or later, Cross Community Access (XCA) profile	XCA supports the means to query and retrieve patient relevant medical data held by other communities. A community is defined as a coupling of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing clinical information via an established mechanism. Facilities/enterprises may host any type of healthcare application such as EHR, PHR, etc.
	IHE ITI-TF Revision 5.0 or later, Cross-Enterprise Document Media Interchange (XDM) Integration Profile	XDM provides document interchange using a common file and directory structure over several standard media. This permits the patient to use physical media to carry medical documents. This also permits the use of person-to-person email to convey medical documents.
	HL7 V3 Confidentiality Codes value set	Confidentiality Code is intended to provide some information about the sensitivity of the data contained in the document to assist systems in determining if the requesting user should be allowed to access the document: N = Normal; R = Restricted; V = Very Restricted

Functionality	Standards	Basic Definition
Service Access	OASIS Simple Object Access Protocol (SOAP) Version 1.2	SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission.
	OASIS Web Services Security:SOAP Message Security 1.1 (WS-Security 2004), 1 February 2006	WS-Security is a communications protocol providing a means for applying security to Web services. NOTE: REST (Representational State Transfer) is not a standard, but an approach to designing software architecture that governs the proper behavior of participants on the Web. REST exemplifies how the Web's architecture emerged by characterizing and constraining the the four components of the Web, namely origin servers, gateways, proxies and clients.
Domain Name Service	IETF: RFC-2181, -2219, -2782. Domain Name Service (DNS) services	The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, *www.example.com* translates to *208.77.188.166* .
Directory Access	IETF: RFC-2251, -2252, -2253. Lightweight Directory Access Protocol (LDAP)	The Lightweight Directory Access Protocol, or LDAP, is an application protocol for querying and modifying directory services. A directory is a set of objects with attributes organized in a logical and hierarchical manner. A simple example is the telephone directory.
	IHE ITI-TF Revision 4.0 or later, Personnel White Pages (PWP)	The Personnel White Pages (PWP) Integration Profile provides access to basic human workforce user directory information. This information has broad use among many clinical and non-clinical applications across the healthcare enterprise. The information can be used to enhance the clinical workflow (contact information), enhance the user interface (user friendly names and titles), and ensure identity (digital certificates).
	RFC 1766 Tags for the Identification of Languages	The language tag always defines a language as spoken (or written) by human beings for communication of information to other human beings. Computer languages are explicitly excluded.