December 2009 - Changes in Data Integrity Standards					
Functionality	**Standards**	**Implementation Timeline**			**Certification Criteria**
		2011	**2013**	**2015+**	
PRODUCT CERTIFICATION STANDARDS					
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)	• 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				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)				Use as guidance in the design and implementation of electronic signatures.
	HIE ITI-TF Supplement Volume 3 – Document Digital Signature (DSG) Content Profile				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.
	ETSI Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)				
	ISO/TS-17090, Health Informatics, Public Key Infrastructure				

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
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)	HIPAA + SHA + AES + TLS	HIPAA + SHA + AES + TLS	HIPAA + SHA + AES + TLS + CMS	• 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. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. • Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
	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				Provide the capability to use AES to encrypt data for transmission.
	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.

	IETF Cryptographic Message Syntax (CMS), RFC-2630, -3852				If an email capability is provided, implement the CMS standard to cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption.