Compliance Summary

	ISO 27001	SOC1	SOC2	SOC3	PCI	HIPAA
Standard	**ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements**	**SSAE18: Statement on Standards of Attestation Engagements No. 18**	**AICPA Trust Services Principles and Criteria, Attest Engagements, Section 101 (AT 101)**	**AICPA Trust Services Principles and Criteria, Attest Engagements, Section 101 (AT 101)**	**PCI-DSS, Payment Card Industry Data Security Standard**	**HIPAA: Health Insurance Portability and Accountability Act of 1996 HITECH: Health Information Technology for Economic and Clinical Health Act of 2009 HIPAA Omnibus 2013**
Owner	**International Organization for Standardization**	**American Institute of Certified Public Accountants (AICPA)**	**American Institute of Certified Public Accountants (AICPA)**	**American Institute of Certified Public Accountants (AICPA)**	**Payment Card Industry Security Standards Council**	**US Department of Health and Human Services (HHS)**
Standard Contents	Design: • Context, • Leadership • Planning • Support • Operations • Performance • Evaluation Controls: • Policies • Organization • HR, Asset, Access • Cryptography • Physical Environment • Operations • Communications • Acquisition, Suppliers • Incidents, Business Continuity • Regulatory/ Contractual compliance	Report of internal controls governing financial reporting: • Security (Physical & Logical) • Availability A subset of SOC2 controls for the same principles. Type 1 tests control design Type 2 tests control operating effectiveness	Report to evaluate information systems across several principles: • Security (Physical & Logical) • Availability • Processing Integrity • Confidentiality • Privacy Audits may cover just security principle or more. Type 1 tests control design Type 2 tests control operating effectiveness	General Use Report (unrestricted) of compliance to AT 101 (SOC2)	Design: • Secure Networks and Systems, • Cardholder Data Protection • Vulnerability management • Access Control • Monitoring and testing • Information Security Policies	• Privacy and Security Controls for Protected Health Information (PHI) Access • HR, Awareness & Training, • Physical, Administrative and Technical Controls • Encryption • Data Transmission & Integrity • Workstation & Media • Business Associates • Data Breach Requirements • Required additional Business Associate Agreement
Audit process	• External Auditor • Renewed Annually	• External Auditor • Renewed every 6 or 12 mon	• External Auditor • Renewed every 6 or 12 mon	• External Auditor • Renewed every 6 or 12 mon	• External Auditor	• Reviewed periodically • Subject to external audit on demand