

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	<p><u>Design:</u></p> <ul style="list-style-type: none"> Context, Leadership Planning Support Operations Performance Evaluation <p><u>Controls:</u></p> <ul style="list-style-type: none"> Policies Organization HR, Asset, Access Cryptography Physical Environment Operations Communications Acquisition, Suppliers Incidents, Business Continuity Regulatory/ Contractual compliance 	<p>Report of internal controls governing financial reporting:</p> <ul style="list-style-type: none"> Security (Physical & Logical) Availability <p>A subset of SOC2 controls for the same principles.</p> <p><u>Type 1</u> tests control design <u>Type 2</u> tests control operating effectiveness</p>	<p>Report to evaluate information systems across several principles:</p> <ul style="list-style-type: none"> Security (Physical & Logical) Availability Processing Integrity Confidentiality Privacy <p>Audits may cover just security principle or more.</p> <p><u>Type 1</u> tests control design <u>Type 2</u> tests control operating effectiveness</p>	<p>General Use Report (unrestricted) of compliance to AT 101 (SOC2)</p>	<p><u>Design:</u></p> <ul style="list-style-type: none"> Secure Networks and Systems, Cardholder Data Protection Vulnerability management Access Control Monitoring and testing Information Security Policies 	<ul style="list-style-type: none"> 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 <p>• Required additional Business Associate Agreement</p>
Audit process	<ul style="list-style-type: none"> External Auditor Renewed Annually 	<p>External Auditor</p> <p>Renewed every 6 or 12 mon</p>	<p>External Auditor</p> <p>Renewed every 6 or 12 mon</p>	<p>External Auditor</p> <p>Renewed every 6 or 12 mon</p>	<ul style="list-style-type: none"> External Auditor 	<ul style="list-style-type: none"> Reviewed periodically Subject to external audit on demand