ABT Medical Data Security

ABT Medical, Inc.

Physical controls include:

- 24/7/365 Armed Security Teams
- Two Factor Authentication
- Biometric Identity Verification at the Equipment Rack Level
- Extensive Use of Video Surveillance

Network and logical controls include:

- Multi-Factor Authentication
- Hardware and Software Firewalls
- Vulnerability Scans
- Anti-Virus and Anti-Spyware Protection
- Intrusion Detection and Prevention Services
- Industry Standard Use of IPSEC, VPN, and SSL Certificates

Compliance Documentation:

HIPAA Compliance

Our data center and cloud infrastructure meet stringent requirements for compliance with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA establishes national standards to protect individuals' medical records and health information and applies to health plans, health care clearinghouses, and those healthcare providers that conduct certain health care transactions electronically. Our data center complies with the rules that apply to our systems and levels of access which helps our clients comply with portions of HIPAA that apply to them.

HITRUST

The HITRUST Common Security Framework (CSF) provides a comprehensive, flexible, and efficient approach to regulatory compliance and risk management. It aggregates existing globally recognized standards, regulations, and business requirements; including ISO, NIST, PCI, HIPAA, COBIT, and state laws into a coordinated security matrix. It is used by healthcare, business, technology and information security leaders to assist in safeguarding health information systems and exchanges.

SSAE-16 SOC 1 Type 2

SOC 1 reports are provided to service organizations that are reporting on controls relevant to Internal Control Over Financial Reporting (ICFR). Type 2 reports sample data over a period of time, providing assurance of consistent compliance, versus using data from just a single point in time with Type 1.

ABT Medical Data Security

ABT Medical, Inc.

PCI DSS v3.2 AoC and Merchant Level 4/SAQ D Certification

The Payment Card Industry Data Security Standard is followed by organizations that store, process, and/or transmit cardholder data. Our data center undergoes quarterly vulnerability and penetration testing through Sysnet Global Solutions.

SSAE-16 SOC 2 Type 2

SOC 2 framework is a reporting option specifically designed for entities such as data centers, I.T. managed services, software-as-a-service (SaaS) vendors, and other technology and cloud computing-based businesses. SOC 2 frameworks address a comprehensive set of criteria known as the Trust Services Principles covering security, availability, system integrity, information confidentiality, and privacy of personal information. Type 2 reports sample data over a period of time versus using a single point in time, providing a more complete and thorough report.

SSAE-16 SOC 3 Type 2

SOC 3 reports are general use reports designed to meet the needs of users who want assurance on the controls at a service organization related to the set of Trust Service Principles covering security, availability, system integrity, information confidentiality and privacy. Like the SOC 2, the SOC 3 provides a service auditor's assessment of the service organization maintenance of effective controls over its system as it relates to these trust principles based on AICPA's AT 101 Attestation standard. It does so without disclosing details about the test descriptions or data assessed. SOC 3 are always Type 2 reports, based on comprehensive data sampling over time rather than using data generated at a single point in time.

SSL Report

Our data center earned an SSL A rating through Qualys SSL Labs. SSL provides for the secure transmission of data and supports the technology behind encrypting sensitive information on the Internet. This provides our customers with security and peace of mind when working in our web applications.

Please contact us if you need more information.