WhiteSpace
HEALTH

WhiteSpace Health Security

Information security is a major concern for all healthcare organizations. Those who elect to outsource key business operation to third-party vendors (e.g., SaaS, cloud-computing providers) have a particular vested interest in their business associate's ability to properly manage data in applications and networks. Even the slightest gaps in network security can leave enterprises vulnerable to attacks, data theft, extortion, ransomware, and malware, causing data to become inaccessible in addition to a PR nightmare. We take security of protected health information (PHI) and other data seriously. That is why WhiteSpace Health's Revenue Intelligence Platform has been certified as SOC2+ compliant.

What is SOC 2+?

AICPA Service Organization Control Reports
AICPA
SOC 2
CERTIFIED
Managed IT Service Provider

System and Organizational Controls (SOC) is a comprehensive reporting framework created by the American Institute of Certified Public Accountants or AICPA. There are two sets of requirements. Type I requirements describe our systems and explain how our design is well suited to meet the relevant trust principles. Type II details the operational effectiveness of our systems.

WhiteSpace Health has designed each of our controls to comply with one or more of the trust principles. Our internal SOC 2+ audit report provides regulators, business partners, suppliers, and others with valuable information about how WhiteSpace Health manages data.

An independent third-party auditor that is governed by AICPA guidelines has assessed our ability to manage customer data based on five elements of the Trust Services Criteria - security, availability, processing integrity, confidentiality, or privacy. In healthcare, SOC 2+ compliance is considered an essential benchmark for SaaS providers.

Security

The security principle refers to protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information. IT security tools such as network and web application firewalls or WAFs, two factor authentication and intrusion detection are useful in preventing security breaches that can lead to unauthorized access of systems and data.

PRIVACY
SECURITY
AVAILABILITY
PROCESSING INTEGRITY
CONFIDENTIALITY
SOC 2
CERTIFICATION

Availability

The availability principle refers to the accessibility of the system, its products, or services as stipulated by a contract or service level agreement (SLA) where the minimum acceptable performance level for system availability is specified by both parties.

The principle of availability does not address system functionality and usability. However, it does involve security-related criteria that may affect availability. Monitoring network performance and availability, site failover and security incident handling are critical.

Processing integrity

Processing integrity clarifies whether a system delivers the right data at the right price at the right time. To ensure processing integrity, data processing must be complete, valid, accurate, timely and authorized.

However, processing integrity does not necessarily imply data integrity. If data contains errors prior to being ingested into the system, detecting them may not be the responsibility of the processing entity. Monitoring of data processing, coupled with quality assurance procedures, can help ensure processing integrity.

Confidentiality

Data is considered confidential if its access and disclosure is restricted to a specified set of persons or organizations. Examples may include data intended only for company personnel, the Health Insurance Portability and Accountability Act or HIPAA, business plans, intellectual property, internal price lists and other types of sensitive financial information.

Encryption is an important control for protecting confidentiality while data is in motion. Network and application firewalls, together with rigorous access controls, can be used to safeguard information being processed or stored on computer systems.

Privacy

The privacy principle addresses the system's collection, use, retention, disclosure, and disposal of personal information should conform to the organization's privacy notice, as well as with criteria set forth in the AICPA's Generally Accepted Privacy Principles (GAPP). Personal identifiable information (PII) refers to details that can distinguish an individual such as name, address, Social Security number, etc. Some personal data related to health, race, sexuality, and religion is also considered sensitive and requires an extra level of protection under HIPAA. Controls must be put in place to protect all PII and PHI from unauthorized access.

The Importance of SOC 2 Audits

Outsourcing is a growing trend and healthcare organizations are becoming increasingly dependent on third party providers to deliver mission critical services. In healthcare, the standard is even higher and business associates must address confidentiality and security along with other compliance and regulatory requirements.

SOC 2 compliance is not a requirement for SaaS and cloud computing vendors. However, the importance of adhering to SOC 2 criteria in securing your data cannot be overstated. WhiteSpace Health undergoes regular audits to ensure the requirements of each of the five trust principles are met and that we continue to remain SOC 2-compliant. Our compliance extends to all services we provide including:

- Web application security;
- DDoS protection;
- Content delivery through CDN;
- Load balancing;
- Attack analytics.

The results of a SOC 2 audit are intended to meet the needs of a broad range of users requiring detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports are created by a neutral auditor, and they play a vital regarding the oversight of the organization, vendor management programs, corporate governance and risk management processes, regulatory compliance oversight, and more.

Purpose and Benefits of SOC 2 Audits

Benefits for Clients and Prospects

- Periodic SOC reports can be useful to shareholders, customers, and other stakeholders to provide assurance on operational integrity.
- SOC reports provide comfort to clients that the servicing organization has appropriate controls in place.
- Comfort is also provided to auditors that there are robust controls protecting financial reporting.
- Assurances of adequacy of controls over data processing and security are conferred in the report.

Benefits to WhiteSpace Health

- Effectiveness of controls that have been put in place are demonstrated.
- Independent verification and monitoring of internally controlled environment.
- Third party audit is accepted by most clients and minimizes disruption caused by additional client audits.

- Identifies and reports areas of weakness and inefficiency.
- Promotes the understanding and openness between WhiteSpace Health and its customers.
- Maintains existing clients and has capability to attract new ones.

About HITRUST

The HITRUST framework supports HIPAA, which is the US government's standard that covered entities such as health plans, clearinghouses, providers, and their vendors (also called business associates) must follow. Covered entities and their business associates must comply with HITRUST standards at all stages of data transmission and storage of health information to ensure its integrity and confidentiality.

- Information Security Program
- Access Control
- Human Resources Security
- Risk Management
- Business Continuity Management
- Security Policy
- Organization of Information Security
- Compliance
- Asset Management
- Privacy Practices
- Physical and Environmental Security
- Communications and Operations Management
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management.

AICPA Combined Certifications

SOC 2+ compliance includes operational items of WhiteSpace Health already covered in SOC 2+ certification. Additionally, SOC 2+ includes topics specific to our unique requirements, including HITRUST, ISO-27001 and NIST. We have combined these audits to consolidate assurance reporting into one report which also helps us control costs. AICPA, our accrediting body, issues the combined certification.