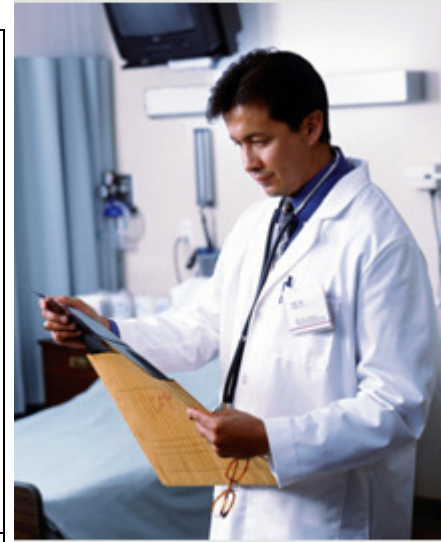


HIPAA Compliance

For more information call SPS at 817-461-3393 or visit www.harding-group.com

SPS was designed to provide HIPAA compliance to Medical Professionals. The following table lists the HIPAA rules that SPS provides compliance for.

Contingency Plan	<p>164.308(a)(7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.</p> <p>164.308(a)(7)(ii) Implementation specifications: (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.</p>	<p>SPS Remote Backup software and services provide a complete, secure solution for the backup, retention, and recovery of data. With CDP (Continuous Data Protection), multi-tiered BLM (Backup Lifecycle Management), and bare metal restore capabilities, data is never more than a couple of clicks away from being fully restored from multiple RPOs (Recovery Point Objectives).</p>
Access Controls	<p>164.312(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).</p>	<p>With SPS Remote Backup software, data access is controlled by centrally managed policies, so only authorized individuals have access to sensitive data.</p>
Audit Controls	<p>164.312(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</p>	<p>SPS Remote Backup allows for logging of data backup, deletion, and recovery activities, which can be monitored for all home and ROBO locations through a centralized management tool.</p>
Data Integrity	<p>164.312(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.</p> <p>164.312(c)(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</p>	<p>To ensure the highest level of data security, the small files and delta blocks of data are first compressed and then encrypted up to AES 256. Data remains encrypted in-flight and at-rest. The backup data is only unencrypted by the DS-Client at the site when it has retrieved the encrypted data. With SPS Remote Backup's BLM, digital certificates are created for data deleted from the database.</p>
Authentication	<p>164.312(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.</p>	<p>With SPS Remote Backup software, users are authenticated by a username and password, so only authorized individuals have access to sensitive data. 128 bit AES Data encryption (including user credentials) and 128 bit SSL provide protection from the possibility of theft of credentials helping to provide a secure and accurate audit trail.</p>



Typical Clients Include:

Hospitals

Clinics

Doctors

Dentists

Orthodontists

Healthcare Facilities

Medical Associations

Nursing Associations

Medical Examinators



The Harding Group Inc.

1250 E. Copeland Rd Arlington, TX 76011

Ph: 817-461-3393 Fax: 817-461-3394