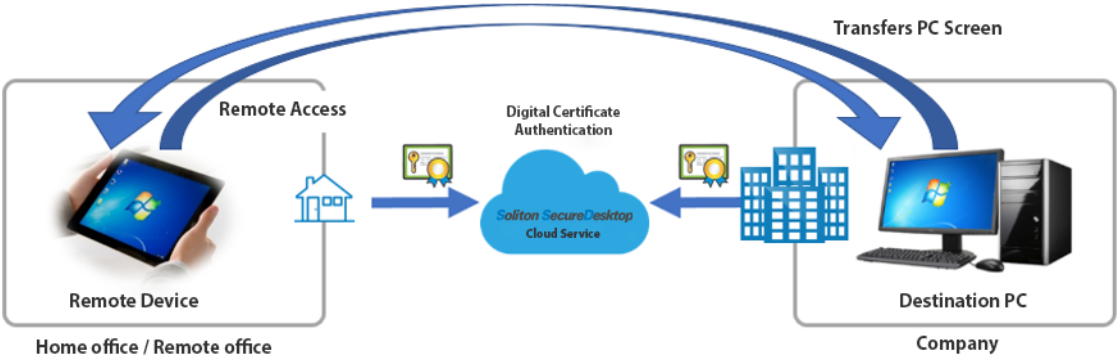
Soliton®

Soliton SecureDesktop



HIPAA Compliance Information

Technical Safeguards

Compliance with HIPAA Technical Safeguards

Category	Required/ Addressable	Standards	How Soliton SecureDesktop Helps
§164.312(a) Access Control	Required	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.	▪ Access to the office computer is protected using two different passwords for authentication. A separate password is used for logging into the client and then to the office computer. ▪ Digital certificates are used for two-factor authentication to prevent unauthorized devices from accessing the office computer. ▪ Access from a device or account can be stopped easily by an administrator.
	Required	Unique User Identification Assign a unique name and/or number for identifying and tracking user identity.	▪ A unique userID/password can be assigned to users by administrators.
	Required	Emergency Access Procedure Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	▪ SecureDesktop enables access to an office computer from anywhere with internet connectivity. It can be used to provide emergency access to health information.
	Addressable	Automatic Logoff Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	▪ Users are automatically logged out for inactivity after a preset time.
	Addressable	Encryption and Decryption Implement a mechanism to encrypt and decrypt electronic protected health information.	▪ TLS (including TLS 1.2) and 256-bit AES encryption is used to secure all remote connections and data transfers.

Compliance with HIPAA Technical Safeguards

Category	Required/ Addressable	Standards	How Soliton SecureDesktop Helps
§164.312(b) Audit Controls	Required	Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	▪ All remote sessions are logged and easily accessible by administrators.
§164.312(c) Integrity	Required	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	▪ Physical access to the office computer is disabled during a remote session to prevent commands/inputs from anyone other than the remote user.
	Addressable	Mechanism to Authenticate Electronic Protected Health Information Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	▪ Only the office computer's screen data is transferred to the client computer. SecureDesktop does not modify any data and only programs on the office computer can modify data. ▪ Decrypted data during a remote session is checked for network transmission integrity.
§164.312(d) Person or Entity Authentication	Required	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	▪ Office computers are protected by strong passwords and digital certificates. Users must login and have an appropriate digital certificate installed to access an office computer.

Compliance with HIPAA Technical Safeguards

Category	Required/ Addressable	Standards	How Soliton SecureDesktop Helps
§164.312(e) Transmission Security	Required	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	▪ All remote connections and data transfer is secured using TLS (including TLS 1.2) and 256-bit AES encryption. ▪ No data can be downloaded to or uploaded from the client computer. ▪ No data is left on the client device after a remote session ends. ▪ Soliton does not store or have access to any health data. The encrypted screen data transmitted during a remote session is not stored.
	Addressable	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	▪ Decrypted data during a remote session is checked for network transmission integrity.
	Addressable	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	▪ TLS (including TLS 1.2) and 256-bit AES encryption is used to secure all remote connections and data transfers.