PROXY Pro Remote Desktop Software and the Health Insurance Portability and Accountability Act (HIPAA)

The Role of PROXY Pro in a HIPAA Compliant Environment

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the main Federal law that protects health information. The HIPAA Privacy and Security Rules protect the privacy and security of individually identifiable health information. HIPAA Rules have detailed requirements regarding both privacy and security.

The HIPAA Privacy Rule covers protected health information (PHI) in any medium, while the HIPAA Security Rule covers electronic protected health information (ePHI).

Although HIPAA compliance per se is applicable only to entities covered by HIPAA regulations (e.g., healthcare organizations), PROXY Pro remote desktop software provides all of the necessary security and privacy features needed for an organization to remain HIPAA compliant while providing remote access.

Security – Technical Safeguards (CFR 164.312)

Technical safeguards mean the technology and the policy and procedures for its use that protect electronic protected health information (ePHI) and control access to it.

CFR Title 45 - Public Welfare is one of fifty titles comprising the United States Code of Federal Regulations (CFR). Title 45 is the principle set of rules and regulations issued by federal agencies of the United States regarding public welfare. **Subchapter C, Part 164 —Security Standards for the Protection of Electronic Protected Health Information**

https://www.ecfr.gov/cgi-bin/text-idx?SID=1f19037d8ee0abb72477851d48233f6f&mc=true&node=pt45.1.164&rgn=div5#se45.1.164_1312

	HIPAA § 164.312	PROXY Pro
(1)	**(a)(1) Standard: 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**	• Create role-based access control policies based on fine-grained permissions (e.g. enable/disable input control, enable/disable file transfer, etc) and apply to specific remote computers or custom defined groups of remote computers • Restrict access to remote computers by IP address, IP address range and/or time blocks • Supports Windows Authentication and Multi-factor authentication (MFA) • Rate-limited password attempt lockout • Custom logout option for Host and Admin sessions • Administrator ability to terminate any session as well as end user ability to do so if configured • Require end user acceptence of remote control session – configurable • Centralized dashboard for monitoring connection status • See our website or contact Proxy Networks, Inc. for a full list of security controls and options

Security – Technical Safeguards (CFR 164.312)

	HIPAA § 164.312	PROXY Pro
(2)	**(a)(2)(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.**	All users are identified by a unique username and password as defined by Windows authentication. Can configure with local Windows accounts, Domain accounts or Azure AD accounts
(3)	**(a)(2)(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.**	PROXY Pro Web Console provides customizable logoff periods for inactivity. The Administrator has full control over this
(4)	**(a)(2)(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.**	All session data is protected with 256-bit AES encryption by default. Administrator can also require SSL communications only.
(5)	**(b) Standard: 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.**	Details of all access to the Web Console and connection related details to any remote machine are logged in a centralized database. Reports for custom time periods can easily be generated. Note that PROXY Pro software does not directly access or modify any health information.
(6)	**(c)(1) Standard: Integrity (Required). Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.**	PROXY Pro provides the ability to suppress keyboard and mouse input on remote machines while a session is in progress. Ability to screen record the session and access to those recordings by a technician is configurable and under complete control of the administrator. Note that PROXY Pro software does not directly access or modify any health information.
(7)	**(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.**	No data, aside from meta-data about the session, is stored. Ability to screen record is configurable. If enabled, content is in a proprietary format placed in a secure location. It is recommended that screen recording not be turned on in order to simplify HIPAA compliance. Note that PROXY Pro software does not directly access or modify any health information.

	HIPAA § 164.312	PROXY Pro
(8)	**(d) Standard: 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.**	Windows Authentication local, domain, or Azure is used to authenticate users. Machines over the open internet will employ a prorpietary "shared-secret" authentication. Connection protocol can be limited to SSL only.
(9)	**(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.**	All network traffic is encrypted using AES 256-bit encryption. Only session audit data is stored. Recording ability can be completely disabled. Note that PROXY Pro software does not directly access or modify any health information.
(10)	**(e)(2)(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.**	All network traffic is encrypted using AES 256-bit encryption. Only session audit data is stored. Recording ability can be completely disabled. Note that PROXY Pro software does not directly access or modify any health information.
11)	**(e)(2)(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.**	All network traffic is encrypted using AES 256-bit encryption. Only session audit data is stored. Recording ability can be completely disabled. Note that PROXY Pro software does not directly access or modify any health information.

For additional help or questions, please give us a call at 1-800-PROXY-US!