HIPAA and VNC Connect

Version 1.2

Contents

What is HIPAA? 3
What guidelines must remote access software follow? 3
Key terminology 4
Notes on VNC Connect's cloud connectivity 4
How does VNC Connect support HIPAA regulations? 4
- Access control (§ 164.312 (a)) 4
  - Unique user identification (Required) 5
  - Emergency access procedure (Required) 5
  - Automatic logoff (Addressable) 5
  - Encryption and decryption (Addressable) 5
- Audit controls (§ 164.312 (b)) 6
- Integrity (§ 164.312 (c)) 6
  - Mechanism to authenticate electronic protected health information (Addressable) 6
- Person or entity authentication (§ 164.312 (d)) 6
- Transmission security (§ 164.312 (e)) 7
  - Integrity controls (Addressable) 7
  - Encryption (Addressable) 7

Conclusion 7

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) mandates that any organization storing, managing or transmitting health care information must protect it sufficiently from unauthorized access. With VNC Connect, your organization can receive the business benefits of remote access software without sacrificing HIPAA compliance.

This document details the security guidelines remote access software must follow when used within an organization seeking HIPAA compliance, and explains how VNC Connect's extensive security features are compatible with these regulations.

Note: The information contained in this document is not legally binding, nor do we intend for it to be used as legal advice. Instead, we recommend providing your auditor with a copy of this document to help your HIPAA audit go as smoothly as possible.

What guidelines must remote access software follow?

HIPAA regulations encompass a broad spectrum of software and hardware. As such, only certain regulations apply to remote access software. These are as follows:

TECHNICAL SAFEGUARDS § 164.312		
Standard	**Section**	**Implementation specifications**
Access control	164.312(a)	Unique user identification (Required) Emergency access procedure (Required) Automatic logoff (Addressable) Encryption and decryption (Addressable)
Audit controls	164.312(b)	
Integrity	164.312(c)	Mechanism to authenticate electronic protected health information (Addressable)
Person or entity authentication	164.312(d)	
Transmission security	164.312(e)	Integrity controls (Addressable) Encryption (Addressable)

Note: Any item marked as 'addressable' is up to the interpretation of your auditor, and whether they feel adequate protection has been implemented in this category.

Key terminology

Throughout this document, we refer to certain RealVNC-specific terminology.

VNC Connect is remote access software consisting of two apps: **VNC Server** and **VNC Viewer**. You must install and license VNC Server on the computer you want to control. This is known as your **VNC Server computer**.

You must then install VNC Viewer on the computer or device you want to take control from, which is known as your **VNC Viewer device**. You do not need to license this device, meaning you can freely connect to your VNC Server computer from as many devices as you wish.

Notes on VNC Connect's cloud connectivity

VNC Connect offers the ability to make remote access connections via RealVNC-managed cloud services ('via the cloud'). During such connections, screen data displaying electronic protected health information may pass through RealVNC's cloud servers. This data is end-to-end encrypted in such a way that RealVNC has no means to decrypt or read it, technical or otherwise. Critically, RealVNC's only interaction with this encrypted data is to transfer it.

For cloud-brokered connections, RealVNC acts as a conduit of information and is a transmission-only service. As such, as per the FAQ listed at https://www.hhs.gov/hipaa/for-professionals/faq/245/are-entities-business-associates/, RealVNC is not considered a 'business associate', and no *Business Associate Agreement* is required.

VNC Connect also allows for *direct* connectivity. For the avoidance of doubt, no cloud services are involved for connections made directly via TCP/IP. For more information, see our paper on cloud vs direct.

How does VNC Connect support HIPAA regulations?

Access control (§ 164.312 (a))

"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 § 164.308(a)(4)."

a. Separate access control lists regulate who can discover computers, who can connect to them, and what they can do once connected.

   - Discovery

     System administrators can use their RealVNC account to control which members of a team can discover which computers. If a user is unable to discover a computer, they cannot connect to it.

   - Connectivity

     System administrators can configure the VNC Server app to determine who has permissions to connect.

     They can also determine which in-session features different users can access (e.g. whether the connection is view only, or if they can transfer files).

b. The VNC Server computer can be configured to query connecting users. This means the local user will be informed of - and must manually authorize - each new connection.

c. If a RealVNC account's security settings (e.g. its password) are altered, an email is automatically sent to the user confirming these changes.

d. System administrators can choose how many authentication failures a user can make before they are blacklisted for a configurable period of time.

Unique user identification (Required)

"Assign a unique name and/or number for identifying and tracking user identity."

a. VNC Server is configured by default to identify users according to their unique system account name (e.g. Windows, macOS or Linux account name).

b. Users are authenticated using system account credentials; either username and password, or multi-factor authentication (see the relevant page on the RealVNC website for details of supported multi-factor schemes).

c. Users can also be authenticated using Single Sign-On / GSS-API compliant mechanisms, meaning connecting VNC Viewer users are transparently authenticated by secure network services (e.g. Kerberos), without having to enter an additional password.

d. RealVNC accounts are identified by email address, which can be uniquely assigned to each user.

e. RealVNC accounts are authenticated using either username and password, or multi-factor authentication.

Emergency access procedure (Required)

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."

a. You can use VNC Connect to remotely access the healthcare information safeguarded by your organization. This means you always have instant access to critical files in an emergency situation, no matter where you are in the world.

Automatic logoff (Addressable)

"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

a. By default, users are automatically disconnected when idle for one hour. System administrators can configure this limit.

b. VNC Server can be configured to automatically log off or lock the computer when a remote control session is disconnected.

c. You can remotely sign out of all VNC Viewer devices. This additionally removes cached data from the Address Book of each VNC Viewer device.

Encryption and decryption (Addressable)

"Implement a mechanism to encrypt and decrypt electronic protected health information."

a. VNC Connect uses the RFB 5 protocol, which mandates the use of modern cipher suites and uses strong cryptography throughout.

b. All connections are protected by 128-bit or 256-bit AES-GCM encryption (depending on your settings and subscription type).

c. All connections have perfect forward secrecy, ensuring they cannot be decrypted now or in the future.

d. Online access to your RealVNC account is protected by mandatory TLS. We follow best practices for secure web development, and our website has an A rating from the Qualys SSL Labs test.

Audit controls (§ 164.312 (b))

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

a. VNC Server writes a full record of all connection activity to the system log, which is stored either locally or on a Domain Controller. A system administrator can configure the quality, quantity and destination of these logs as part of their audit procedure.

Integrity (§ 164.312 (c))

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

a. System administrators can determine which in-session features different users can access (e.g. whether the connection is view only, or if they can transfer files, etc.).

b. System administrators can similarly disable the keyboard and mouse input on the VNC Server computer during a connection, preventing unauthorized local data input during a remote session.

c. Audit logs can be used to review who had remote access to machines containing sensitive electronic health information, and to verify that alteration or destruction of data was executed by an authorized user.

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."

a. The VNC Server computer can be configured to query connecting users. This means the local user is informed of - and must manually authorize - each new connection.

b. VNC Server writes a full record of all connection activity to the system log, which is stored either locally or on a Domain Controller. A system administrator can configure the quality, quantity and destination of these logs as part of their audit procedure.

Person or entity authentication (§ 164.312 (d))

"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

See also measures listed under *Unique User Identification*

a. No default password is provided for any RealVNC service.

   In order to connect via the cloud, the user must first specify a RealVNC account password. We recommend this password is unique, and additionally recommend the use of a password manager such as Keypass.

   If the RealVNC account password *is* compromised, the malicious third party remains unable to connect. This is because each VNC Server computer also has its own unique password. By default, VNC Server is protected by system authentication, which mandates that the connecting user must enter the details they usually use to *log in* to that computer. If a malicious third party attempts to guess this password (via

a brute force or dictionary attack), they are blacklisted after five unsuccessful attempts. The system administrator can configure this number.

b. The VNC Viewer app, which is used to take control of remote computers, can be protected with a master password.

c. By default, guest access to computers is disabled.

d. VNC Connect supports two connection types: cloud and direct. If the user chooses, they can disable either.

e. Any data stored by RealVNC is locked behind unique and secure passwords.

f. To see which multi-factor authentication mechanisms RealVNC uses, please visit the relevant page on the RealVNC website.

Transmission security (§ 164.312 (e))

"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

a. It is possible to transmit healthcare information via remote access (e.g. via text chat or file transfer). A system administrator can disable each of these features.

Integrity controls (Addressable)

"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

a. VNC Connect uses the RFB 5 protocol, which mandates the use of modern cipher suites and uses strong cryptography throughout.

Encryption (Addressable)

"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

a. All connections are protected by 128-bit or 256-bit AES-GCM encryption, depending on your settings and subscription type.

b. All connections have perfect forward secrecy, ensuring they cannot be decrypted now or in the future.

c. Online access to your RealVNC account is protected by mandatory TLS. We follow best practices for secure web development, and our website has an A rating from the Qualys SSL Labs test.

Conclusion

You should provide this document to your auditor during your HIPAA audit. This will help ensure your organization meets the appropriate requirements for HIPAA compliance while using VNC Connect remote access software.

Please note this document details only *HIPAA-specific* security features, and VNC Connect does far more to ensure the safety of its users than is described here. For a full overview of VNC Connect security resources, please visit realvnc.com/connect/security.

If you have any questions about the topics raised in this paper, please contact us at privacy@realvnc.com.

RealVNC's remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

Copyright © RealVNC Limited 2016. RealVNC and VNC are trademarks of RealVNC Limited and are protected by trademark registrations and/or pending trademark applications in the European Union, United States of America and other jurisdictions. Other trademarks are the property of their respective owners. Protected by UK patents 2481870, 2491657; US patents 8760366, 9137657; EU patent 2652951. 09Apr2018

www.realvnc.com