REALVNC

HIPAA and the VNC SDK

Version 1.1

Contents

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 the VNC SDK, 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 the VNC SDK'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.

Notes on VNC Cloud

The VNC SDK offers the ability to make remote access connections via RealVNC-managed cloud services ('VNC 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 VNC Cloud 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.

The VNC SDK also allows for direct connectivity ('direct TCP'). For the avoidance of doubt, no cloud services are involved for direct TCP connections. For more information, see our paper on cloud vs direct.

How does the VNC SDK 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. For VNC Cloud connections, access control lists regulate who can attempt to connect. For direct TCP connections, the developer can filter connections by IP address to achieve the same effect.

   For either connection method, the developer can grant permissions based on the authenticated user ID of the person connecting (certain users can be denied access entirely). The developer can look up appropriate permissions using a mechanism of their choice.

b. Developers can ensure successful and failed connection attempts are appropriately recorded in audit logs.

Unique user identification (Required)

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

a. The developer can configure the VNC SDK to require an authenticated user ID before remote access is established. Without this configuration, all connections are rejected by default.

b. The developer can tell the VNC SDK where to find an up-to-date list of authorized user IDs. This ensures unauthorized users do not gain access. It can also restrict users to access during certain times.

c. Developers have full control over how many authentication failures a connecting user can make before being locked out.

d. Public versions of the VNC SDK allow authentication by user ID and password/passphrase.

   Contact RealVNC for information on APIs that will allow multi-factor authentication by a range of different mechanisms.

e. Developers can configure the VNC SDK to meet any password length/complexity requirements, and to enforce any password change policy.

Emergency access procedure (Required)

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

a. You can use remote control apps created using the VNC SDK 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. Contact RealVNC for information on APIs that will allow remote control sessions to be terminated after a period of inactivity ('idle timeout').

Encryption and decryption (Addressable)

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

a. The VNC SDK uses the RFB 5 protocol, which mandates the use of modern cipher suites and uses strong cryptography throughout. Developers can use the VNC SDK's logging functionality to verify cipher suites in use.

b. All connections are protected by 128-bit AES-GCM encryption.

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

d. Access to the VNC Developer online portal is protected by mandatory TLS. We follow best practices for secure web development, and our website is graded A in 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. A developer can configure the VNC SDK to audit any quality of logging, to any destination.

Integrity (§ 164.312 (c))

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

a. A developer 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. 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. A developer could use the VNC SDK to query the ID of each connecting user and present this information to the owner of the computer, enabling the latter to manually accept or reject each connection.

b. A developer can configure the VNC SDK to audit any quality of logging, to any destination.

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."

a. The developer can configure the VNC SDK to require an authenticated user ID before remote access is established. Without this configuration, all connections are rejected by default.

b. The developer can tell the VNC SDK where to find an up-to-date list of authorized user IDs. This ensures unauthorized users do not gain access. It can also restrict users to access during certain times.

c. Developers have full control over how many authentication failures a connecting user can make before being locked out.

d. Public versions of the VNC SDK allow authentication by user ID and password/passphrase.

   Contact RealVNC for information on APIs that will allow multi-factor authentication by a range of different mechanisms.

e. Developers can configure the VNC SDK to meet any password length/complexity requirements, and to enforce any password change policy.

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 the VNC SDK (e.g. via remote control or by copying and pasting between endpoints). These features are disabled by default and must be explicitly enabled by the developer, who can then limit their use to certain users.

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. The VNC SDK uses the RFB 5 protocol, which mandates the use of modern cipher suites and uses strong cryptography throughout. Developers can use the VNC SDK's logging functionality to verify cipher suites in use.

Encryption (Addressable)

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

a. All connections are protected by 128-bit AES-GCM encryption.

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

c. Access to the VNC Developer online portal is protected by mandatory TLS. We follow best practices for secure web development, and our website is graded A in 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 the VNC SDK.

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

www.realvnc.com