How Splashtop Supports HIPAA Compliance

September 2019

HIPAA Compliance

Every business that is part of the U.S. healthcare industry must comply with Federal standards regulating sensitive and private patient information. In addition to protecting worker health insurance coverage, HIPAA sets forth standards for protecting the integrity, confidentiality, and availability of electronic health information.

While no single product or solution can make an organization HIPAA-compliant, the Splashtop remote access products for business, when used properly, can help organizations meet HIPAA guidelines for the privacy and security of remote access to healthcare information and can be used within a larger system to support HIPAA compliance.

Splashtop does not process, store, or have access to any of the users' computer data such as patient data or medical records. Splashtop transmits but does not store the screen capture stream, which is encrypted end-to-end. User passwords are secured in transit and at rest. Authentication consists of multiple levels, including device authentication, the available two-step verification, and various device-level passwords. Our cloud security modules continuously monitor for and block suspicious activities in real-time. Splashtop adopts industry's best practices for protecting both the cloud infrastructure and user data through a combination of encryption, firewalls, virtual private networks, and runtime intrusion detection and defense. The subsequent sections provide more technical details. All of these measures help ensure that Splashtop may be securely deployed in your organization without affecting HIPAA compliance.

Splashtop makes the following remote access products for business use:
Splashtop Business Access (cloud, for remote access)
Splashtop Remote Support (cloud, for remote support)
Splashtop On-Demand Support (cloud, for remote on-demand support)
Splashtop Enterprise (on-premise, for remote access)

Although HIPAA compliance per se is applicable only to entities covered by HIPAA regulations (e.g., healthcare organizations), the technical security controls employed in these Splashtop products meet various HIPAA technical standards. Furthermore, the administrative configuration and control features provided by these Splashtop products support healthcare organization compliance with the Administrative and Physical Safeguards sections of the final HIPAA Security Rules.

The following table is based upon the HIPAA Security Standards rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule).

All implementation standards or specifications marked with a capital "(R)" are required, while those marked with a capital "(A)" are considered "addressable," essentially meaning that the entity is allowed some flexibility in taking "reasonable" steps to comply with the standard or specification to which it refers.

Table: How Splashtop supports HIPAA security standards

NIST Special Publication 800-66[1]. Descriptions. HIPAA Safeguard. R=Required / A=Addressable	
Security Requirements	**Relevant Features in Splashtop Business Access, Splashtop Remote Support, Splashtop On-Demand Support, and Splashtop Enterprise**
Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. [164.312(a)(2)(i)]	Allows the administrator to assign unique user ID/password to individual user. User IDs can be disabled/deleted.
Person or Entity Authentication (R): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. [164.312(d)]	Mandatory device authentication ensures compromised ID credentials cannot be used from non-authenticated devices. Administrator can choose to approve all device authentication requests. Optional two-step verification further ensures identity of the user. Devices can further require Windows/Mac user credentials or separate security code upon connection. Non-admin users are blocked from modifying streamer security settings and other configuration options.

Access Control (R): 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). [164.312(a)(1)]	Access permissions can be set individually for each user. Users can be grouped for easier management of access permissions. Administrator can allow each user or user group to access specific computers and/or groups of computers. Administrator can disable remote functions such as file transfer, remote print, copy/paste, and session recording. (These functions are by default enabled. We recommend that you disable them via the management console.) Login can authenticate against Active Directory (*Splashtop Enterprise only*). Prevent access from remote locations by restricting access to the local network only (*Splashtop Enterprise only*).
Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. [164.312(a)(2)(iii)]	Idle timeout ensures idle remote sessions automatically disconnected after specified timeout.
Audit Controls (R): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronically protected health information. [164.312(b)]	All remote sessions are logged, including timestamp, user ID, device name, IP address, and session duration. All file transfers performed through the Splashtop file manager are also logged. Remote sessions currently in-progress are marked as such.

Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. [164.312(a)(2)(iv)] Transmission Security (R): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. [164.312(e)(1)] Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. [164.312(e)(2)(ii)]	Splashtop does not process, store, or have access to any of the users' computer data such as patient data or medical records. Splashtop transmits but does not store the screen capture stream, which is encrypted end-to-end. The entire remote session including the screen capture stream and keystrokes are secured with TLS (up to 1.2) and AES 256-bit encryption. Splashtop user credentials are protected in transit via HTTPS/TLS (up to 1.2). Splashtop user passwords are stored securely as salted hashes on encrypted server disks. Code signing of Splashtop software eliminates the possibility of tampering. There is the option of uploading your organization's own SSL certificate for additional security (*Splashtop Enterprise only*).

For further details and to start a free trial, please visit:

Splashtop Business Access (cloud, for remote access)

Splashtop Remote Support (cloud, for remote support)

Splashtop On-Demand Support (cloud, for remote on-demand support)

Splashtop Enterprise (on-premise, for remote access)

Splashtop Security Features

Splashtop's business products are specifically built to give IT teams full control over securing the data while giving employees the flexibility to access their authorized computers from anywhere. They are especially applicable to organizations operating in industries with stringent legislative and compliance regulations where controls for data privacy and systems security are mandated.

- **Industry standard encryption**: Encrypts all data end-to-end using TLS (up to 1.2) with AES 256-bit encryption.
- **Device authentication**: Devices used to remotely access computers must be authenticated via the stored email addresses.
- **Multi-level password security**: Log in with Splashtop ID/password. Optionally, enforce OS password or custom security code.
- **Two-step verification/two-factor authentication**: Use an extra mobile device-based authentication method to further guarantee identity.
- **Blank screen:** Automatically blank the screen while a remote session is active.
- **Screen auto-lock:** Automatically lock the OS screen after a remote session ends.
- **Session idle timeout:** Disconnect remote sessions after no activity for specified time.
- **Remote connection notification:** Notify user with an on-screen message when a remote user connects in, eliminating "stealth connections."
- **Copy/paste control:** Administrator has the option of disabling copy/paste. (Copy/paste is by default enabled. We recommend that you disable it via the management console.)
- **File transfer control:** Administrator has the option of disabling file transfer. (File transfer is by default enabled. We recommend that you disable it via the management console.)
- **Remote print control:** Administrator has the option of disabling remote print. (Remote print is by default enabled. We recommend that you disable it via the management console.)
- **Session recording control:** Users can initiate session recording during a remote session. Administrator has the option of disabling the session recording capability. (Session recording is by default allowed. We recommend that you disable it via the management console.)
- **Lock streamer configuration:** Non-admin users are blocked from changing streamer security settings and other configuration options.

- **Digitally signed applications:** All software shipped by Splashtop is digitally signed to ensure it is not improperly altered.
- (*Splashtop Enterprise only*) **Active Directory integration**: IT administrators can create and authenticate users based on AD.
- (*Splashtop Enterprise only*) **MDM/MAM integration:** Integration with MDM/MAM partners adds additional on-device security and control.
- (*Splashtop Enterprise only*) **SSL Certificates:** For additional security, the administrator and mobile users import existing SSL certificates signed by a Certificate Authority (CA) or can generate new, self-signed certificates.

Company Information

Splashtop Inc. delivers the best-in-class remote access and remote support experience.

Splashtop Inc. is headquartered in San Jose, California.

For further details and to trial Splashtop products, visit www.splashtop.com.

Splashtop Inc.
1054 S. De Anza Blvd., Suite 200
San Jose, CA 95129, U.S.A.
+1.408.861.1088