How Splashtop Helps Support HIPAA Compliance

April 2017

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 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 makes the following remote access products for business use:
Splashtop Business Access (SaaS, for remote access)
Splashtop Remote Support (SaaS, for remote support)
Splashtop On-Demand Support (SaaS, 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)] 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)] 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)] Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. [164.312(a)(2)(iii)]	Allows the administrator to assign unique user ID/password to individual user. IDs can be disabled/deleted. Access permissions can be set individually for each user. Administrator can allow each user to access specific computers and/or groups of computers. 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. Non-admin users are blocked from modifying streamer security settings and other configuration options. Idle timeout ensures idle remote sessions are not left connected. Streamers can authenticate via proxy servers to help prevent password capture, replay attacks, and spoofing. Authenticates and verifies IDs against Active Directory

	(*Splashtop Enterprise only*). Restrict access from remote locations by limiting access to the local network only (*Splashtop Enterprise only*).
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)]	Maintains an audit trail of all remote sessions, including user ID, device name, session duration, and timestamp. A real-time view of sessions is also displayed.
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)]	Uses TLS with AES 256-bit encryption end-to-end so user data is protected during transmission. Restricts cipher suite to 2048-bit ECDHE-RSA with 256-bit AES-CBC and SHA1. Code signing of Splashtop software eliminates the possibility of tampering. Option to upload company SSL certificates for additional security (*Splashtop Enterprise only*).

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

Splashtop Business Access (SaaS, for remote access)
Splashtop Remote Support (SaaS, for remote support)
Splashtop On-Demand Support (SaaS, 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 it 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 with AES 256-bit encryption.
- **Device authentication**: Devices used to remotely access computers must be authenticated.
- **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 authentication method or device 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:** Splashtop Business Access, Splashtop Remote Support, and Splashtop On-Demand Support support copy/paste. Administrator has the option of disabling it.
  (Splashtop Enterprise does not support copy/paste.)
- **File transfer control:** Splashtop Business Access, Splashtop Remote Support, and Splashtop On-Demand Support support file transfer. Administrator has the option of disabling it.
  (Splashtop Enterprise does not support file transfer.)
- **Remote print control:** Splashtop Business Access and Splashtop Remote Support support remote print. Administrator has the option of disabling it.
  (Splashtop On-Demand Support and Splashtop Enterprise do not support remote print.)
- **Lock streamer configuration:** Non-admin users are blocked from changing streamer security settings and other configuration options.
- **Proxy Server authentication:** Splashtop streamer supports Basic and NTLM authentication with a proxy server using HTTPS to help prevent password capture, replay attacks and spoofing.

- **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, cross-screen productivity and collaboration experience, bridging smartphones, tablets, computers, TVs, and clouds. Splashtop remote desktop services enable people to remotely access their computers from anywhere, using any device.

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