How Splashtop Helps Support HIPAA Compliance

October 2013

Table of Contents

1. HIPAA Compliance

The Mobile/BYOD revolution is here to stay. Each day, as new devices are released to the market, they are brought into your company and onto the corporate network by employees who use them to access everything from corporate email to line of business applications locked inside highly customized IE browsers.

But if you are like most CIOs, CSOs and IT managers responsible for network security, you're spending countless nights worrying about the security ramifications. One of the biggest challenges most companies face is how to allow mobile devices to access confidential patient data in a secure manner that doesn't impact the users productivity AND helps you meet HIPAA guidelines for the privacy and security of healthcare information.

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, Splashtop® Business and Splashtop Enterprise products 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.

Although HIPAA compliance per se is applicable only to entities covered by HIPAA regulations (e.g., healthcare organizations), the technical security controls employed in Splashtop business meet various HIPAA technical standards. Furthermore, the administrative configuration and control features provided by Splashtop business 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	**Splashtop Business and Enterprise Security Features** *** - Indicates Splashtop Enterprise feature only**
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 a unique user id/password (ID) to individual users. IDs can be edited or de-activated/deleted. * Authenticates and verifies IDs against Active Directory.
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)]	* Grouping allows users access to groups of physical or virtual desktops on a per user and group basis. * Device authentication ensures compromised ID credentials cannot be used from non-authenticated devices. * Restrict access from remote locations by limiting access to the local network only. * Restrict access using MAC address filtering on desktops and mobile devices * Force password entry for every session by removing automatic login option from remote device.
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)]	* Non-admin users are unable to override configuration options. Streamers can authenticate against proxy servers to help prevent password capture, replay attacks and spoofing. * Idle timeout ensures sessions are not left logged in.

Security Requirements	Splashtop Business and Enterprise Security Features * - Indicates Splashtop Enterprise feature 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 connections including the devices connecting from/to, session duration, date and time of session. 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 SSL/AES-256 bit encryption for the end to end communication so customer health information is protected during transmission. Restricts cipher suite to 2048 bit ECDHE-RSA with 256-bit AES-CBC and SHA1. Code signed components of the software eliminate the possibility of tampering. * Option to upload company SSL certificates for additional security.

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

Trial Splashtop Enterprise
www.splashtop.com/enterprise

Trial Splashtop Business
www.splashtop.com/business

2. Splashtop Security Features

Splashtop products were designed and created by a team of security and networking experts, leveraging cutting-edge encryption and authentication technologies. Our SaaS and on-premise products are specifically built to give IT teams full control over securing the data while, at the same time, 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 SSL / AES 256-bit.
- **Active Directory integration**: IT administrators can create and authenticate users based on AD.
- **Blank screen:** Automatically blank the screen while a remote session is active. The admin can optionally force the blank screen for each session.
- **Screen auto-lock:** Automatically lock PC after the remote session ends to ensure the PC is not left logged in after a remote session terminates.
- **OS-level Access Control:** Optionally enforce controls already in place on the corporate LAN.
- **Session idle timeout:** Logout users when session has no activity for a specified time.
- **Remote connection notification:** Notify users on the desktop systems when a remote user connects to the PC with an on-screen message, eliminating “stealth connections”.
- **Copy/paste prohibited:** Prohibit remote user from copying/pasting information to/from the desktop
- **File transfer prohibited:** Prohibit remote user from transferring files to/from the desktop.
- **Disable remote auto-login:** Force password re-entry for every remote connection.
- **Hide streamer configuration:** Non-admin users are unable to view/change configuration options.
- **Invalid SSL certificate warning:** Warning displayed if the SSL certificate is invalid.
- **Proxy Server authentication:** The Splashtop streamer supports Basic and NTLM authentication with a proxy server using HTTPS to help prevent password capture, replay attacks and spoofing.
- **Digital signed applications:** All software shipped by Splashtop is digitally signed so nothing can be altered or updated by any individual without the private key.
- **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.
- **MDM/MAM integration:** Deep integration with MDM / MAM partners adds additional on-device security and control.

3. Company Information

About Splashtop

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 access and control their favorite apps, files, and data via their mobile devices. More than 15 million people have downloaded Splashtop products from app stores, and manufacturing partners including HP, Lenovo, Dell, Acer, Sony, Asus, Toshiba, AMD, Intel and others have shipped Splashtop on more than 100 million devices. Splashtop Inc's headquarters are in San Jose, California.

For further details and to start a free trial, visit www.splashtop.com/enterprise or www.splashtop.com/business

---

Silicon Valley Headquarters
1054 S. De Anza Blvd, Suite 200
San Jose, CA 95129
U.S.A
+1.408.861.1088

Taipei Office
10th Floor, No. 222,
Fuxing South Road, Section 1,
Taipei, Taiwan, 10666
+886.2.2778.0706

Tokyo Office
Level 20 Marunouchi Trust Tower
- Main
1-8-3 Marunouchi, Chiyoda-Ku
Tokyo 100-0005 Japan