mediplay®

Your personalized **ad-free** patient education and marketing network.

Security Overview

Mediplay provides a dynamic educational and marketing program displayed on a monitor in the waiting room or exam room. A client selects videos that are most relevant to the practice(s) and then the programming is enhanced with user-created custom content such as provider bios, practice messages, sales call to action, etc.

Mediplay maintains a vast library of medically related content which is distributed to a network of media players utilizing Mediplay's content management platform. Organizations can select topics, add additional personal content and can update their on-screen message through Mediplay's web portal, Mediplay Connect. Mediplay's web portal sends instructions through a secure API to our content platform partner's cloud based servers, which in turn, distributes the appropriate content to each media player as it checks in for regular updates.

Our platform partner Broadsign International is a leading producer of digital signage network management software. Its software product, the Broadsign Suite, contains important networking and security features to prevent unauthorized viewing or manipulation of sensitive data distributed throughout the network and does not create, store or in any way access EPHI and so does not need to be on a network governed by the Security Rule of the HIPAA. If cost dictates that it needs to run on a network that contains EPHI, security policies can be implemented on the network-level and operating system level to ensure 100% HIPAA compliance.

HIPAA Security Rule and Compliance

The provisions of HIPAA 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the HIPAA Security Rule, apply to electronic protected health information (EPHI) and compliance is the responsibility of the health care provider. Broadsign software does not create, store or access EPHI and does not naturally fall under the regulations of the HIPAA Security Rule.

HIPAA only becomes a factor for Broadsign software when a media player running Broadsign software resides on a network that has access to EPHI data. The HIPAA Security Rule dictates that servers and PCs containing EPHI data only be accessible through secure authenticated and encrypted means with the assumption that a network containing EPHI is accessible to distrusted systems.

Therefore a PC (media player) running Broadsign software does not represent a new threat vector on the network. That being said, it is good IT policy to ensure Broadsign software conforms to IT security requirements.

- All communication is encrypted via SSL
- There is no inbound communication to the media player. For security reasons the server will never attempt to initiate a connection into a network. It is always the media player that initiates the communication to the server (port 10799 and 10805).
- All communication is outbound to a trusted server, the identity of which is cryptographically verified.
- It is also possible to use a web proxy server if the Client do not want to open ports 10799 and 10805 for external access.
- It is possible to designate specific times where the media player can use the network.
- File integrity verification is performed to detect tampered or corrupt media files and prevent their distribution throughout the network. The integrity of files are verified by calculating a checksum on every media file that is imported into the system.
- Mutual authentication is performed between Server and Player. This being said, the Player authenticates itself to the Server and the Server authenticates itself to the Player in such a way that both parties are assured of the others' identity.
- The media player software can be run in a dedicated mode to prevent access to the playback PC's file system.