VIPatient

Security Standards

Security for our customers and their patients is one of our top priorities. To help ensure everyone has the best and most secure experience using VIPatient, we have compiled our security standards to document how we are keeping sensitive data safe.

The VIPatient web application uses SSL security certificates with a 4096 bit encryption to verify that you and your patients are connected securely to our servers.

After the connection is made, the next security protocol in place is our password policy. We require a password that is at least 7 characters long, containing upper and lower case letters as well a numbers. We also engage users to choose longer passwords and are able to remove some of the restrictions the longer your password is.

After logging in, all patient information is stored in a SQL database only accessible from our web servers. VIPatient uses a PBKDF2 one way password hash with a unique salt value for every user every time they change their password.

Our video framework leverages the latest in WebRTC technology. Video calls use an end to end encryption based on a 4096 bit SSL certificate. Most of the time, data is never passed to our servers. In some cases, video information must pass to our control server, located at control.vipatient.net where video information is never decrypted and passed straight to the client.

Our signaling server also uses a trusted SSL certificate to ensure that all communications are secure before they leave the client side browser.

Outline of major security points:

- Trusted SSL (4096 bit) Certificates on all servers
- PBKDF2 Password hash with unique salt values
- SQL server only available to web server