UNDERSTANDING CaseViewNet® SECURITY

CaseViewNet supports wired, wireless, and Internet streaming connections.

CaseViewNet transmits and receives in a HIPAA compliant way.

CaseViewNet secures those connections in the following ways:

1. 256-bit encrypted SSL.
2. WPA/WPA-2 Protocol Network Password
3. Optional Client Password when communicating over Local Area Network (LAN)
4. Mandatory Client Password when using CaseViewNet Cloud over Wide Area Network (WAN)

CaseViewNet Local Area Network (LAN)

CaseViewNet communicates with the Case CATalyst® software over any network connection without the need for file sharing or the opening of special ports. CaseViewNet uses SSL port 443. All reporters licensed to use CaseViewNet over a (LAN) have received a personal 1024-bit SSL certificate signed by Stenograph. All data transferred between Case CATalyst and the CaseViewNet client software is encrypted with AES-256 over an SSL connection.

CaseViewNet Cloud Wide Area Network (WAN)

CaseViewNet Cloud communicates with Case CATalyst and any other Computer Aided Transcription (CAT) software without the need for file sharing or the opening of special ports. CaseViewNet Cloud uses standard SSL port 443. All data transferred upstream to the CaseViewNet Cloud server and downstream to the CaseViewNet client is encrypted with AES-256 over an SSL connection. Transcript data is relayed through the CaseViewNet Cloud server while the realtime session is active. Once the session is terminated by the reporter, all transcript data on the CaseViewNet Cloud server is destroyed. When using CaseViewNet Cloud, it is required that each CaseViewNet client know the specific CaseViewNet Cloud Session Code and connection password to establish a connection.