UNDERSTANDING CaseViewNet® FOR MAXSCRIBE SECURITY

CaseViewNet for MAXScribe supports Internet streaming connections.

CaseViewNet transmits and receives in a HIPAA compliant way.

CaseViewNet for MAXScribe secures those connections in the following ways:

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

CaseViewNet Cloud Wide Area Network (WAN)

CaseViewNet Cloud communicates with MAXScribe 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.