Understanding CaseViewNet security

When it comes to understanding security within CaseViewNet, most court reporters that provide the realtime and the legal professionals receiving it are really just looking for assurances that the data is secure. If that description fits you, you can rest assured that CaseViewNet provides security in the following ways:

1. 256-bit encrypted data stream over SSL, some of the strongest encryption available (commonly used for banking transactions over the internet)
2. Optional WPA protocol to secure and password-protect your network router
3. Password controlled user rights that limit the viewing and saving of the realtime file

For IT professionals and those who want to know more, here are the details:

CaseViewNet is one of the most technically advanced interactive litigation programs available today. It supports both wired and wireless connections, and offers multiple ways to secure your data stream as well as your realtime file.

Network Connection

CaseViewNet communicates with Case CATalyst® over any network connection without the need for any file sharing or the opening of special ports. All CaseViewNet clients will have received a personal 1024-bit SSL Certificate signed by Stenograph. All data transferred between the Case CATalyst server and CaseViewNet is encrypted with AES-256 over the SSL connection established with this certificate.

If you choose to use 802.11 Wi-Fi technology, it is optional to secure your wireless network using the WPA protocol. With this security established, clients wishing to connect to the reporter's personal network would need to know, in addition to the CaseViewNet password, the password that the reporter created for the router. This gives you peace of mind that other programs and file shares are secure. But again, this is not necessary for CaseViewNet since the realtime data stream is always protected.

A wired connection to the court reporter's router with a CAT5/CAT6 Ethernet cable is also available if a wireless connection is not an option. Connecting CaseViewNet through an Ethernet cable connection offers all of the same great CaseViewNet features and functions as a wireless connection; such as RapidRefresh that updates all of the reporter's edits, and the ability to receive the entire realtime file even if connecting and joining late.

File Protection

In a Case CATalyst CaseViewNet network, Case CATalyst is the realtime server. Each connecting client computer will need a password from the reporter in order to sign on to the reporter's Case CATalyst server to receive the realtime feed. The court reporter protects his/her realtime file with the use of these passwords to limit user rights. The reporter can limit each client's ability to view the realtime file or view and save the realtime file. Passwords also determine whether or not you have rights to save the realtime file, marks and annotations and copy text; or rights to generate a report for only the marks and annotations. The court reporter can also specify the expiration dates of these passwords to limit access to the realtime feed. User rights are displayed at the bottom of the client's CaseViewNet screen and can be changed by the court reporter at any time.