

Is Quantum CNS's information protected and secure?

Your data is safe with Quantum CNS. We are committed to your data security and all Quantum CNS solutions run in a secure, world-class hosting facility with system redundancy, fail-safe power systems, 24x7 on-site monitoring and full database backup.

What hardware and software are required to use Quantum CNS?

No special software is required to run Quantum CNS. All that is needed is a PC running Windows XP or higher with 512MB of RAM, a current browser, and a high-speed internet connection allowing for anytime, anywhere connectivity.

How do users access Quantum CNS?

The Quantum CNS Application is accessed via high-speed internet using a web browser to our secure site. Supported browsers include IE 6.0 and higher, Mozilla Firefox 2.0 and higher, and Google Chrome. Quantum CNS can only be used by validated users with current Quantum CNS usernames and passwords.

Does Quantum CNS encrypt data and what type of encryption is used?

Yes, the entire Quantum CNS application uses secure SSL 128-bit encryption for data transmission.

Is the Quantum CNS network reliable?

The Quantum CNS network is comprised of a Multi-Gigabit network backbone with over 5.6 Gbps bandwidth across 5 geographically diverse data centers utilizing multiple providers to deliver Internet access (Level3, Time Warner Telecom, Savvis, RCN, GNAP, and MCI/Uunet). We have available burstable bandwidth from 10 – 1000 Mbps; private point to point connectivity through preferred telcos 1.5 Mbps – 1Gbps and redundant network connectivity available via HSRP and BGP. As a managed load balancing operation, the Quantum CNS network can accommodate up to 2000 SSL transactions per second.

Is there a firewall in place?

Yes. There is a 24x7 managed dedicated firewall (OpenBSD Platform). Among the firewall features: stateful filtering; packet shaping, queuing and prioritization; 25GB traffic log retention; 100,000 Simultaneous Connections, 25 IPsec VPN Routes to Interoperable Gateway; and 100 OpenVPN VPN Client Connections.

Is Quantum CNS a Critical Clinical System?

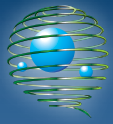
No

What is the data classification?

EPHI

Is my stored data safe?

Client data is stored at a secure audit-certified data facility. Data is stored on redundant servers and is backed up automatically. Data restore can be initiated only by authorized Quantum CNS personnel. A comprehensive contingency plan is documented and in place. Additional information and documents can be provided on request.



What type of data backup plan is in place?

All backups are monitored 24x7 and are performed disk-to-disk-to-tape within a backup window to ensure completion. One weekly full backup retained on tape for 30 days and six incremental backups per week each retained on tape for 14 days are performed; all backup data is available during committed retention period.

Does Quantum CNS have a documented disaster recovery plan?

Yes

Does Quantum CNS provide security awareness training for its users?

Yes

In an emergency, can Quantum CNS bypass user security to provide access to the application?

Yes. Only Quantum CNS System Administrators have access to all areas of the system and direct access to the database.

Does the Quantum CNS application suspend or terminate after a prescribed amount of inactivity?

Yes. Quantum CNS will time out after a period of inactivity. This time interval can be customized based on the client's security needs.

Is there removable media created for backups? How is it stored? What is the procedure to remove EPHI from media before reuse?

Yes. Quantum CNS has extensive audit capability. All user login attempts are logged, whether successful or not and the IP address is recorded. All user actions within the system and against the database are logged. Administration-level users with proper security permissions can view these logs. QuantumCNS adheres to all HIPAA compliance protocols.

Does Quantum CNS use user directories for authentication or to access control? (storing role or access control information in groups inside the directory)

No

Does Quantum CNS have unique user ids for each user?

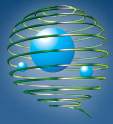
Yes. Generic user ids are not permitted in Quantum CNS. All users have assigned IDs.

What is Quantum CNS's password policy? (password format, length, rotation period, # of tries before lockout, # grace logins)

Quantum CNS requires passwords of 5-50 characters and should include a combination of uppercase, lowercase letters and numbers. Passwords expire every 60 days. (The expiration length can be customized by client.) The system remembers the last 5 passwords used and prevents repetition of them.

Who is authorized to make changes to user accounts in Quantum CNS?

Only users with appropriate Administrative level permissions can access and update other users permissions and roles. All users can update their own passwords.



How are permissions and roles defined within the Quantum CNS application?

Access levels and permissions are based on roles in Quantum CNS. There is a comprehensive and customizable array of roles available to allow users the appropriate access levels they need to the Quantum CNS application. Each user may be assigned to one or multiple roles. Since Quantum CNS adheres to HIPAA compliance protocols, it is recommended that user roles and permissions be assigned on a “need to know” basis.

What are the minimum rights required to run Quantum CNS?

Local User

Does the Quantum CNS Application use the network user id?

No

Do physicians use Quantum CNS?

Yes. Physicians with a valid QuantumCNS user name and password can use the system. All users have access to QuantumCNS modules based on user hierarchical rights.

What other groups of users use Quantum CNS?

Doctors, nurses, QA personnel, administration - anyone involved in improving performance and quality with a valid user name and password can use Quantum CNS.

How can data be sent to Quantum CNS?

Data can be sent to Quantum CNS by secure encrypted web transmission, remote scanning, HL7 interface, and scheduled automatic batch file transmissions.

Is my data safe if I choose to enter my Quantum CNS documents using remote scanning?

Quantum CNS uses Datacap Taskmaster software loaded on your local PC which stores and forwards your uses full 128 bit SSL encryption of the data post scanning and prior to transmission of the CQI data. (note: additional hardware and software is required)

How is my transmitted data protected if I elect to populate my Quantum CNS records electronically?

All data transmitted to and from Quantum CNS is encrypted using SSL 128-bit encryption. If an HL7 interface is used, the channel works over a secure VPN connection between the client and our secure data facility. If batch file transmission is used, the files are FTPd to Quantum CNS from the client over a secure VPN and sent automatically using secure FTP to our secure data center.