

## CERECONS Security

CERECONS has created significant structure to provide for the protection of secured customer data and also follow the security framework as specified by HIPAA. For CERECONS, security is a priority that is based on the importance of protecting our client's data in physical and network environments. The result is a consistent policy and practice across the organization focused on securing the data and its access.

With CERECONS, among the security measures offered include:

- Updated deployment of security technologies
- Evaluation of new security threats and developments
- Commitment to a secure, private, collocated system at our data center
- Proven, current firewall protection, SSL encryption, and other security offerings

Our production systems are located in Irvine, California at a secure data center that provides 24-hour security, limited authenticated access, redundant power supplies and cooling equipment, and other resources to maintain a continuously running system.

The network is protected by a firewall and monitored by intrusion detection software and logging. The CERECONS team monitors the production server logs to check for changes, new vulnerabilities, and other threat assessments. Data encryption using a 128-bit VeriSign SSL Certification is employed with a lock symbol visible on the browser throughout the secured session visit.

User authentication is handled only with a verified username and password under the SSL encryption. A unique cookie is used to verify the session on the specific machine being used with the security model being used for each user session. This authentication also applies to system accounts for database and operating system by employing strong passwords and not using master passwords across systems.

Operating and related application software is kept maintained with recommended service patches and updates as needed to maintain the appropriate system security. Removal of unneeded protocols, ports, default users, and running processes are also done to minimize opportunities for security vulnerabilities.