ClientTrack® by eccovia

DATA PROTECTION & SECURITY

Eccovia's network protection includes network isolation, virtual networks, communication encryption, and site-to-site and point-to-site VPNs. All network protection begins with limiting physical access to the network environment, including physical security of Tier I assets.

The Power of Azure

Hosted in Microsoft Azure, ClientTrack's databases are protected with state-of-the-art security, providing protection against threats such as distributed denial of service (DDoS), Azure backups and Azure Site Recovery to ensure your data is recoverable in disaster scenarios, and easier compliance with external privacy standards, laws, and regulations, including GDPR, HIPAA, ISO 27001, HITRUST, and FERPA. ClientTrack leverages 256-bit SSL and TLS 1.2 encryption both in transit and at rest, so your data remains safe wherever and however you access ClientTrack.

User Security

ClientTrack's security features for user accounts include the following:

- ClientTrack hashes all passwords within the database
- Automatic time out after a set period of inactivity
- Concurrent login prevention of the same user account
- Username and strong password requirements plus automatic password renewal
- Ability for local admins to customize features related to password expiration and reset, login attempts, and lockout time

User accounts are automatically deactivated after a period of inactivity and passwords automatically expire after a pre-defined period of time.

Role-based Security

ClientTrack is built to manage role-based security and data sharing. ClientTrack allows you to segment and partition data by user, program, organization, and other data types as defined by your local administrators, so no user can see client data that doesn't pertain to their role. Additionally, all data is exported with 256-bit Advanced Encryption Standard (AES). With ClientTrack, you have the peace of mind of knowing your data is always safe and secure.