

PhDx Systems Security White Paper

PhDx Corporate Offices

Physical Security

PhDx offices are located in an office complex with after-hours security patrols and coded access to the building. Within the building, PhDx has restricted access and within the PhDx office spaces, access to the computer facility is restricted to authorized personnel and is located behind doors with multiple locks. Access to the servers supporting clients is monitored by the director of network administration and is restricted to authorized computer personnel only.

System Security

Microsoft Active Directory controls user accounts and users are only given access to authorized resources on the network. Password aging and complexity rules are in place and enforced.

All servers are backed up daily using the current Disk-to-Disk technology. Backup disks are rotated on a weekly daily cycle and stored off site to a secure location in Albuquerque. In addition to the daily backups, image backups of all critical systems are performed on a monthly cycle and also stored offsite.

Firewall and Anti-Virus systems are in place to protect the computer environment from outside intrusion attempts. Monitoring software informs system administrators of any current problem.

The computer facility has dedicated electric circuits, separate environmental controls, and battery operated UPS systems.

PhDx Data Center

PhDx hosts our production software and databases at a leading provider of managing hosting services. A summary of the physical and system security services are outlined below.

Physical Security

- Data center limited access
- Biometric scanning for controlled data center access
- Security camera monitoring at all data center locations
- 24x7 onsite staff provides additional protection against unauthorized entry
- Unmarked facilities to help maintain low profile
- Physical security audited by independent firm

System Security

- Branded hardware systems
- System patching configured to provide ongoing protection from exploits
- Dedicated firewall and VPN services to provide additional layer of protection against unauthorized system access

Real Data. Real Outcomes. Real Time.

- Optional, dedicated intrusion detection devices to provide an additional layer of protection against unauthorized system access
- Distributed Denial of Service (DDoS) mitigation services based on proprietary system
- Anti-virus software to provide protection against new and unknown threats
- Risk assessment and security consultation by professional services teams
- Monitoring software informs system administrators of any problem that may arise

Data Transmission Security

Data sent over the Internet during a browser session is encrypted using Secure Sockets Layer (SSL) with a 128-bit certificate provided by VeriSign

Application Authentication

PhDx uses individual login/password combinations to authenticate a user. Once a secure web session has begun, the client is immediately prompted for their application ID and password. Failure to supply valid responses will deny the client access to the PhDx application.

Application Security

Application security utilizes a role-based scheme based on the combination of permissions determined by an individual login identifier and membership in one or more user group(s). Read and/or write access to data, and specific application functionality can all be restricted based on user-level and group-level permissions. Individual read/write/functionality permissions can be granted based on a user's login ID.

Data Backups

Production servers are backed up on a nightly basis. Client data is encrypted and backed up to tape media in addition to it being backed up to a secure offsite location nightly. In addition a transaction log backup is performed every 30 minutes. Tape media is stored in a secure location and rotated offsite weekly. Backup tapes and disks are securely destroyed when their useful life expires.