



## PhDx Systems Security

The security of sensitive healthcare data is an important issue when selecting an application service provider. The security measures at PhDx are multi-layered to address many different aspects of the clinical study management process – data security and back-up, security of data transmitted over the Internet, network security, physical access to computer facilities and software application security.

### *HIPAA Compliance*

<http://www.phdx.com/security.html>

### *PhDx Data Center*

PhDx hosts our 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 access limited to data center technicians
- Biometric scanning for controlled data center access
- Security camera monitoring at all data center locations
- 24 x 7 onsite staff provides additional protection against unauthorized entry
- Unmarked facilities to help maintain low profile
- Physical security audited by an independent firm

#### *System Security*

- System installation using hardened, patched OS
- System patching configured to provide ongoing protection from exploits
- Dedicated firewall and VPN services to help block unauthorized system access
- Dedicated intrusion detection devices to provide an additional layer of protection against unauthorized system access
- Anti-virus software to provide protection against new and unknown threats
- Risk assessment and security consultation by professional services teams

#### *Authentication*

PhDx uses Class 3 Secure Server certificates granted by VeriSign, a recognized digital certificate authority. Server certificates identify a web server to client browsers wishing to establish an encrypted HTTPS web session. Client certificates are assigned to a specific client by a certificate managing authority. Client certificates serve to identify a given client browser to a specific web server. PhDx is capable of creating, assigning and managing its own client certificates in order to identify incoming requests to our web server.

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 login ID and password. Failure to supply valid responses to either field will deny the client access to the PhDx application.



### ***Data Transmission Security***

Data sent over the Internet during a browser session is encrypted using Secure Socket Layers (SSL). PhDx establishes secure web sites (accessed by a URL beginning with HTTPS to host all client databases.

### ***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. A user login identifier and password are assigned to each user of the PhDx® Health Information Platform. Individual read/write/functionality permissions can be granted based on a user's login ID.

### ***Data Backup Procedures***

PhDx uses standby servers with backups of client data to minimize recovery time in the event of hardware failure. In addition all client data is encrypted and backed up nightly on tape media.

### ***Physical Security at PhDx***

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 to areas that process and store protected health information.