PHRAnywhere℠

How is the PHRAnywhere Data Populated and Protected?

The information contained in PHRAnywhere comes from insurance carriers, plan administrators, pharmacy benefit managers, laboratories and diagnostic centers. Encrypted data flows through multiple interfaces from each specific system to the central database. These interfaces exchange data at periodic intervals. Data is then transferred from the central database for display on the secure website.

Any time medical information is stored electronically there may be concerns about patient privacy. PHRAnywhere has taken steps to ensure the storage of health information is secure and complies with all government and HIPAA regulations, including:

- PHRAnywhere stores all data in a SAS70, Type II certified facility.
- PHRAnywhere is a web-based architecture with the business logic located separate from the data.
- PHRAnywhere web server authentication is achieved using 128-bit server-side certification (issued by VeriSign).
- PHRAnywhere utilizes a unique user-authentication process controlled by the user.
- Provider offices are given “levels” of access to information based upon specific job function and need. For example, a receptionist may only have access to demographic and insurance information, not medical records or health summaries.
- Employers are never given access to a member’s specific medical record or health summary.
- Access to health information is strictly controlled by the member.