

TeleRehab™ VersaCare

ScottCare fully supports your clinic's HIPAA compliance.

Any healthcare organization or company that deals with protected health information (PHI) must ensure that all the required physical, network and process security measures comply with the Health Insurance Portability and Accountability Act (HIPAA). Companies and healthcare institutions—not products—are required to comply with HIPAA regulations. Products can only support your ability to comply with those regulations through specialized features.

The VersaCare system incorporates core features that assist with HIPAA compliance, including:

- **User authentication and authorization** to manage information flow, identify users with varying access control levels and restrict activity access (creating, viewing or changing record information) based on the user profile.
- **Auto-lockdown security** that automatically locks down the operating system to essential services. After a select period of inactivity, VersaCare also automatically removes access to PHI and logs out.
- **Audit trail security** tools that log key user parameters such as data access and transfers, login/logouts, and network associations.
- **Electronic signatures**
- **Secure transmission** of electronic order data in HL7 format, including diagnoses, test results, observations, billing information and reports.






These same tools and services provide dual support because they also help improve workflow and ease access of information.

As you consider VersaCare, rest assured that ScottCare is uniquely positioned to facilitate and support your cardiopulmonary rehabilitation department's compliance with HIPAA. For more information on the VersaCare system and its HIPAA-related software features, please contact your ScottCare sales representative at 800.243.9412 x 116.








Standard with Every VersaCare System

21 CFR Part 11 System Requirements

Audit Trails

- Generate Secure Records of Transaction 
- Record Date, Time, Identity and Transaction 
- Prevent Signature of Record from Being Altered 
- Time-stamp of Record Must Reflect Local Time 
- Store Initial Raw Data from Instrument 




Security

- User Name and Password 
- Prevention of Duplicate Passwords 
- Historical Record of Controlled Transactions 
- Prevention of Falsifying Electronic Signatures 
- Authority Checks to Verify Permitted Access 
- Automatic Notification of Inappropriate Access 
- Automatic Time-Outs After Inactivity 

Electronic Record Systems

- Advanced Report Generating Capability 
- Display Data Electronically and by Hard Copy 

Signature Specifications

- Identity Must Be Clear and Unambiguous 
- Signature Must Include Data and Time 
- System Must Identify Transaction 
- Signature Must Be Immediately Available 