EndoWorks® 7

Endoscopy Information Management Solution

Data Security

Today, healthcare providers often collaborate electronically, sharing critical patient information through technology like e-mail, EMR, and Web-based applications. This leaves organizations with the challenge of safeguarding Electronic Protected Health Information (EPHI) from various internal and external risks. EndoWorks 7 provides two levels of security for your organization to choose from: basic and advanced. You determine the level of security that's best for you and configure your system accordingly.

What is basic security?

With basic security, the EndoWorks server validates the user ID and password with those assigned in the EndoWorks database. This user account information, defined via the User Maintenance screen, is managed by the local EndoWorks system administrator.

What is advanced security?

With advanced security, the user is authenticated by comparing the user ID and password with the user information stored in an internal or external repository on the eTrust™ Embedded Identity and Access Management server. The administrator continues to maintain the user account in EndoWorks. The information defined in EndoWorks is shared with either the internal or external repository. If the EndoWorks system is configured for internal advanced security, the administrator has read/write privileges to manage the user's profile; if configured for external advanced security, the administrator is granted "read" privileges only and cannot change the user's profile.

Why do I need a password?

Using a system password prevents transmission of system security to unauthorized entities or persons. Upon logging into the EndoWorks application, your password is validated according to the type of security (basic or advanced) and business rules in effect on the system. In basic mode, the default value is alphanumeric, 1-20 characters in length. In advanced mode, the default value is alphanumeric and the length is determined by the system settings specified in the centralized password management. Regardless of the security mode, the password must not contain leading or trailing spaces.

If internal advanced security exists on the system, the EndoWorks system administrator can set password policies such as preventing passwords from being the same as the username or locking the account after a set number of failed log-ins.

If external advanced security exists on the system, the user ID and password are maintained by the customer's IT department. This ensures that EndoWorks meets all security requirements of the facility.

Data Security EndoWorks 7

The details on Advanced Internal Security

Standard Features

User Management

1. Define start/end dates of staff (User account access automatically enforced outside of defined time frame)
2. Reset users' passwords
3. Force users to change password at next login
4. Suspend accounts

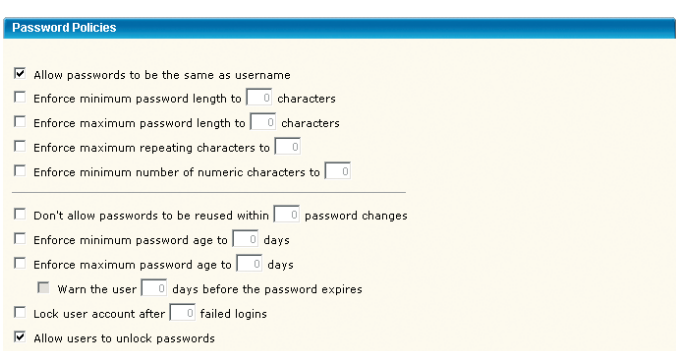
Password Management

1. Enforce password strength rules
   - Min/Max length
   - Max repeating characters
   - Min numeric characters
   - Prevent reuse of old passwords
2. Automatic enforcement of password change timing
   - Min/Max password age
   - Advanced warning to users
3. Lock out users after configurable failed login attempts

Help with HIPAA compliance

Enhanced audit trails with reports for

- Login attempts
- Password changes



The details on Advanced External Security

Optional Features

LDAP Interface

1. Single sign-on: Log on to EndoWorks using the same Username/Password as other applications
2. Pre-configured settings for the following LDAP implementations
   - CA eTrust™ Admin
   - Microsoft® Active Directory®
   - Novell® eDirectory™
   - Sun™ ONE Directory
3. Custom LDAP Mapping available