Biometric Authentication for Allscripts EHR
Compliant Two Factor Authentication for EPCS

Allscripts Gold Partner

Biometric Authentication

Enterprise EHR

Sunrise CM

Professional EHR

Key Benefits

- **Convenience**
  Increases clinician satisfaction, encouraging greater meaningful EHR use
- **Productivity**
  Streamlines workflow efficiency, giving doctors and staff more time for patient care
- **Greater Security**
  Protects patient and staff data, and provides an indisputable audit trail of all actions

Key Features

- Integration with Allscripts workflow for seamless, non-intrusive use
- Intuitive graphical interface for quick and easy registration and authentication
- Unique 40+ level fingerprint image enhancement filters guaranteeing both low false match and false reject rates
- Multi-layer, triple encryption to prevent fraudulent capture or replay of fingerprint data

ID Director for Allscripts EHR

With BIO-key's ID Director, providers simply swipe a finger on a reader for advanced authentication and secure access to Allscripts EHR - without cumbersome passwords or expensive technology. Providers use any approved device - workstation, laptop, tablet or smartphone - and they can be authenticated across any secure network from any approved location, even from home. ID Director can strengthen security, fully address regulatory requirements for advanced authentication and improve user satisfaction and efficiency. Pre-integrated with all Allscripts EHR solutions and with demonstrated success in practice, clinic and hospital settings, ID Director is the right choice for advanced authentication.

Business Challenge: How to achieve Convenience *and* Security

Accurately authenticating each EHR user at sign-on is absolutely essential for protecting patient data and preventing system misuse, but sign-on is only part of the challenge. In a typical healthcare setting where many people may have access to the workstation, laptop or other device running the EHR application, every critical action and transaction should be properly authenticated. The challenge for health care organizations is balancing security with convenience for busy physicians and other EHR users. Passwords, which can be stolen or inappropriately shared, provide inadequate protection. They're also cumbersome to remember and inconvenient to use; adding additional keystrokes to access information or complete a task can actually discourage meaningful EHR use, especially if password entry is required multiple times in the course of a patient encounter. Using an advanced authentication method beyond passwords is the best way to protect private PHI data and prevent EHR system misuse. In fact, advanced authentication is already required by DEA for e-prescribing of controlled substances and is expected to be required for remote network access to all personal health information by 2015 under the Stage 3 EHR incentive program.

Solution - BIO-key ID Director: Authentication - Anywhere

More Protection for the Allscripts EHR and Patient Data: The key measure of any authentication method is the false acceptance rate (FAR) - the likelihood of erroneous authentication. In recent, independently verified National Institute of Standards and Technology testing, BIO-key exceeded the DEA's FAR standard by a factor of 10 - or less than one in 10,000! And, unlike passwords, a fingerprint can't be borrowed and used by another provider, so utilization can be appropriately managed and accurately tracked and audited.

More Convenience for Providers: With ID Director the entire process - from finger swipe to authentication - takes about two seconds. That's at least six seconds less than it takes to enter and authenticate a strong password. Fingerprint verification is triggered automatically by the Allscripts EHR workflow, which presents the authentication dialog box at the pre-determined point in the workflow, so the user never has to initiate an authentication request, deviate from the normal business process or leave the Allscripts EHR screen.

30 DAY REPORT

Real-time Performance Report
Top Hospital ePrescription Department

251,447 EPCS Authentications 99.34% First Swipe Acceptance

Differentiators

- Highest independently-tested and verified NIST scores for fingerprint identification speed and accuracy
- Pre-integration with all Allscripts EHR solutions for risk-free implementation
- Full compliance with DEA two-factor requirements and approved by State Board of Pharmacy
- Plug-and-play support for virtually all fingerprint readers from every major manufacturer
- Reader interoperability so a user can enroll on one device and authenticate on any other device or reader in any authorized location or facility
- Availability on workstation, laptop, tablet and Smartphones

Supported Environments

Servers

Windows Server 2003 or greater
SQL Server 2005 or greater

App Servers

Apache
TomCat
JBoss
IIS
WebLogic
Cold Fusion
And many more

Simple Enrollment and Fast, Secure & Compliant Authentication

Allscripts EHR users interact with BIO-key's ID Director at initial enrollment and whenever advanced authentication is required.

Enrollment

Through an initial, one-time enrollment process - either on the user's workstation or at a central enrollment location - the provider's finger is scanned from any one of 50 plus supported readers. Prompted by an enrollment dialog box in the Allscripts EHR, the provider simply places the appropriate finger on the reader and the finger biometric information is instantly collected.

The finger image is digitized and the data encrypted and converted to a mathematical template representing the features of the fingerprint. BIO-key's patented image processing technology uses more than 40 levels of image enhancement to create a highly discriminate template. This process significantly reduces the possibility of a false acceptance or false rejection response during authentication. Before adding the template to the enrollment database, ID Director checks to verify that there is no prior enrollment of that user name with a different template for the same finger. The enrollment template cannot be converted back into a finger image, so the fingerprint itself can never be reproduced and misused.

Authentication

After initial entry of both a user name and fingerprint at sign-on, a finger swipe provides a simple, easy and convenient way to access individual patient records, complete prescriptions and approve clinical notes. The data extracted from the finger scan is used to build a reference template, which is then matched against the user's enrollment template based on a patented BIO-key algorithm comparing over 1,200 data points. The user is then notified of successful authentication - usually within a second.

Just as in the enrollment process, any one of more than 40 plus fingerprint readers from over 30 manufacturers can be used for capturing the fingerprint - including embedded readers available with many laptop and notebook models and inexpensive portable USB readers. Unique to ID Director, the reader used for enrollment doesn't have to be the same used for authentication, and different types of readers can be used on different devices or at different sites. ID Director also supports readers available for specific Apple and Android tablets and smartphones.

Intuitive User Interface Template

Customizing the prompts, buttons, background colors and other visual elements of the enrollment and authentication dialog boxes to make it a seamless extension of the Allscripts EHR system.

DEA & State Board of Pharmacy/Compliant Authentication for EPCS

The most convenient way to meet two-factor compliance regulations of the DEA and State Board of Pharmacy for Electronically Prescribed Controlled Substances (EPCS) is BIO-key's ID Director.

BIO-key International, Inc. • 3349 Highway 138 • Building D Suite A • Wall • New Jersey • 07719
www.bio-key.com • 866.846.2594