

LOCATION

Dartmouth, MA

OVERVIEW

Faced with strict new password policies for the Medical Records System (MRS), Hawthorn Medical implemented DigitalPersona's fingerprint authentication solution for its 100+ physicians and medical assistants working in their Urgent Care and primary medical facility. Fingerprint authentication has streamlined access to the MRS as well as assisted with HIPAA regulatory compliance mandates for securing patient data.

NEEDS

Secure, convenient and auditable access to the Medical Records System containing patient data.

DIGITALPERSONA PRODUCTS

DigitalPersona® Pro Workstation

DigitalPersona® Pro Kiosk

DigitalPersona® Pro Server



Hawthorn Medical



digitalPersona®

Security Challenge

Hawthorn Medical uses a Longitudinal Medical Record (LMR) application to enter patient data into its hosted Medical Records System (MRS). Physicians and medical assistants use multiple passwords to gain access to confidential patient data and scheduling on the MRS.

The need to remember various passwords was time intensive and cumbersome resulting in weak passwords that did not comply with MRS policies nor HIPAA regulations. In addition, the MRS did not time out or lock when someone stepped away allowing for patient data to be exposed in exam rooms.

Knowing that the MRS would soon implement stricter password policies making it even harder for physicians and medical assistants to remember, Hawthorn Medical decided to search for a secure, convenient authentication solution that would provide strong administrative controls.

Hawthorn Medical needed a solution that could accommodate and track multiple users on notebook and workstation PCs.

DigitalPersona Solution

After evaluating various solutions, Hawthorn Medical selected DigitalPersona Pro due to its Active Directory integration and ability to set group policies for different departments and users. In addition, DigitalPersona Pro supports notebooks with embedded fingerprint readers that physicians were using in exam rooms.

With DigitalPersona Pro Server, the network administrator is able to control user access to multiple areas within the MRS.

Benefits

- **Productivity** - Allows physicians to see more patients now that they do not spend time retrieving forgotten passwords.
- **Administrative Control** - Network administrator creates password policies for user groups.
- **Compliance** - Provides audit trails to assist with HIPAA regulations.

The Results

DigitalPersona Pro provides authorized physicians and medical assistants with immediate access to patient data allowing for additional patients to be seen every day. Patients no longer have to wait while physicians call the MRS help desk to retrieve forgotten passwords.

"DigitalPersona's solution eliminates the need for physicians to remember passwords," said John R. Tomawski, network administrator for Hawthorn Medical. "The time saved allows for more patients to be seen, a significant benefit for both physicians and their patients."

The major benefit for the IT Department has been the ability to set group password policies for different departments and users. "Securing access to the MRS has allowed us to comply with the new password policies," said Tomawski. "In addition, DigitalPersona Pro provides an audit trail needed for HIPAA regulations."

About DigitalPersona

DigitalPersona is the leading provider of biometric authentication solutions for enterprise networks, developers and consumer OEMs. Founded in 1996, the company designs, manufactures and sells flexible solutions that improve security and regulatory compliance while resolving password management problems. DigitalPersona's fingerprint readers utilize superior optical fingerprint scanning technology to more accurately authenticate users regardless of finger placement. The company's interoperable biometric software solutions uniquely support the industry's widest array of notebooks with fingerprint readers. DigitalPersona's award-winning technology is used worldwide by over 30 million people in the most diverse and challenging environments.