biometric authentication

susquehanna health system

Biometric authentication system to protect sensitive medical data

The Susquehanna Health System in the USA is an alliance of three regional hospitals that has been using the Soarian Clinicals and Soarian Financials hospital solutions with a fully integrated workflow for years now.

As the healthcare sector places particularly high demands on IT security, access to Soarian is now governed by a highsecurity component, the biometric authentication system ID Center. After ID Center had proved its practical worth as security solution in its initial 500-user configuration in 2002, the Susequhanna Health System rolled out the biometric solution throughout the whole organization: all the clinical and administrative staff now use their fingerprints for authentication.

The project

The project encompasses:

▶ ID Center for biometric authentication for clinical applications and the billing system

▶ PC mouse with built-in fingerprint sensor for 3000 users in 3 hospitals

▶ Installation of the software on a high availability cluster system

▶ Taking live and training

▶ Support for hospital staff during the enrollment phase

The aim of the project was to provide protection for sensitive medical data in the context of access to the clinical information system. At the same time, the project laid the basis for genuine verifiability and traceabilty as required by law, since a fingerprint furnishes unambiguous proof of a person's identity. Biometric security technologies are ideal when it comes to complying with strict security regulations.

Atos

IT solves problems
Business Technology prevents them

The solution

All the clinical staff, nurses and physicians as well as all the administrative staff – a total of 3,000 persons in all three hospitals – now use their fingerprints for authentication when accessing a multitude of applications. Depending on their access rights, users will find different applications on their desktops, from workflows for patient registration to clinical programs, patient reports, nursing care plans to drug dispensary. Additional security measures – for example, renewed fingerprint-based authentication for the dispensing of special drugs – are easy to implement. It took the users only a few weeks of fullscale operation to become familiar with the new authentication method.

ID Center needs 1 to 1.5 seconds to identify 90 % of the users, and 2 to 3 seconds to identify the remaining 10 %. The high IT administration cost attributable to forgotten passwords is declining steadily, while the hospital staff gains valuable time to attend to their patients.

Benefits for the Susquehanna Health System

▶ Protection of sensitive medical data is guaranteed as access is granted to authorized staff only.

▶ Security gaps that might be harmful to patients are avoided as it is no longer possible to pass on passwords or grant access to unauthorized delegates.

▶ Basis for genuine verifiability and traceability as required by law.

▶ Savings in IT costs, significant reduction in the number of helpdesk calls made due to forgotten passwords.

Benefits for employees

The employees benefit above all from the added ease of use and comfort afforded to them: they can access a variety of applications without having to memorize any passwords at all. Given the wealth of high-responsibility medical tasks, this eases the strain on hospital staff while improving security at the same time.

Susquehanna Health
The art of caring. The science of healing.