A consistent identity management scheme not only helps to reduce IT support costs, but it also prevents unauthorized access to sensitive information and IT applications. These systems provide many employees and external partners with access to highly sensitive and personal data that must not get into the wrong hands!

Protect Sensitive Data by Controlling Access to Data and Systems Processing Medical, Healthcare and Administrative Information

Today, patient data is even more sought after than credit card data for theft and abuse, as it offers unique insights that cannot be locked or changed. This makes it a prime target. The more IT is used to manage the work of family physicians, labs and hospitals, the more data is generated as a result.

Thieves of healthcare data is of interest to criminals for a number of reasons, ranging from billing fraud through to identity theft. The resulting damage caused is substantial, making it all the more important to protect this data by means of an access management system.

42.5% of all cases of data abuse take place in the healthcare sector.* Over the past two years, 91% of all healthcare companies reported at least one case of data abuse.*

*Identity Theft Resource Center
Increased Data Security Thanks to Optimized Access Protection Based on the Need-To-Know Principle

- Meet compliance regulations relating to confidential healthcare data in accordance with the network and information security (NIS) regulations of the EU, US HIPAA, General Data Protection Regulation and Section 203 of the German Penal Code relating to medical professional secrecy as well as the protection of medical data from unauthorized/administrator access.
- Achieve security through consistent monitoring of user rights assignment – from the request all the way to the technical implementation in the IT system.
- Role-based access authorization helps to ensure the required level of access protection in hospitals and delivers added efficiency. Each user is assigned precisely the access rights to the data and applications actually required to perform their daily work.
- Employees frequently move from one department to another. The resulting required update of access rights can be performed automatically by the respective application, thus greatly improving the security level of patient data.
- Digital request and administrative processes so simple, your specialist department users can operate and configure them. Quickly and securely configure individual access rights to current patient records and results from diagnostics using authorization-based workflows.
- Self-service functions ease IT department workload: Implement a centralized password management system with mobile and e-mail PIN to increase password security and reduce helpdesk costs.
- Cover future requirements by connecting IAM systems to medical devices or new Internet of Things (IoT) applications in the healthcare industry.
- Improved support at the point of care: Control access to electronic patient case records during physicians’ ‘digital rounds.’
- Business intelligence-based reports and analyses allow you to rapidly identify high-risk areas as regards data access.
- Integrate all IT systems with a centralized user management solution. This entails anything from applications such as the hospital information system all the way to standard IT systems such as the Microsoft Active Directory service.
- Connect your identity management and HR management systems to keep all employee data up to date and avoid inconsistencies.

Cyber Crime in the Healthcare Sector

- According to KPMG, 81% of all major hospitals and health insurance providers were subject to data leaks in the past two years.
- More than 50% of the attacks in the healthcare sector originated from insiders.
- 112 million medical records were stolen in the U.S. in 2015.
- For 36% of the affected people, this resulted in financial damage.
- Ø profit of $20,000 per medical identity information unit, i.e., 10x the yield of stolen credit card data.
- Compared to credit card data, it takes 2x as long to discover medical data fraud.