PASSWORD SAFE

IT security in the healthcare sector

The importance of reliable and highly encrypted access management has increased more in the healthcare sector in recent years than in almost any other industry. The reasons for this include the introduction of the General Data Protection Regulation (GDPR) and various reports of cyber-attacks and data theft. In addition, data access in the healthcare sector is often confronted with particularly high requirement profiles and regulations such as critical infrastructure protection (CRITIS). In order to avoid unnecessary burdens for employees in hospitals, clinics and medical practices, we have developed Password Safe, a central solution for the simple and secure management and use of all types of access data.

Intelligent and secure solutions for the healthcare sector

Password Safe supports you with a password management solution tailored to your individual needs. Regardless of whether you are dealing with branched authorisation structures for hospitals or central password management in medical practices: Rely on our extensive experience and long expertise in the IT security industry!

> **Save time and money and work with the market leader in password management right from the start**

Password security without limits

Whether next to a terminal, patient tablet, or hospital information system (HIS), access to all credentials is centralised and cross-device via the web application. Passwords can also be securely shared across sites, wards and platforms - even with external parties. This ensures shorter processing paths and greater efficiency in workflows.

Compliance with security standards

To provide special protection to critical infrastructures (CRITIS) such as hospitals and structures for inpatient care, drugs & vaccines and laboratories, clearly defined access rights are essential. Thanks to the zero-knowledge principle in Password Safe, passwords can even be shared without knowing them in plain text.
In addition, each employee receives only the access rights that are necessary for his daily work - within the required time frame. Unauthorised persons are automatically locked out by RBAC.

Security first

The topic of data security is of immense importance, especially in the healthcare sector. Due to the daily handling of sensitive patient data, it must be ensured that this data is protected and can only be viewed by authorised persons. Central authorisation management for access data including two-factor authentication, PKI and single sign-on helps you meet this requirement.

By storing a second factor for logging in at the workplace, for example, the password is combined with the employee card. Using single sign-on, employees can log on to websites automatically after a one-time authentication process - eliminating the need for manual logon. In accordance with the Patient Rights Act, the documentation of all accesses also makes it possible to prove when, to whom and for what reason access to personally identifiable information (PII) was granted.

Hospital Future Act to promote your IT security

With the Hospital Future Act (HFA), the Federal Ministry of Health has been providing funding for hospitals since 2021-01-01, to support you in digitisation and also IT security measures. According to the HFA, atleast **15 percent of the funding granted must be used for measures to improve information security.**

Eligible IT or cybersecurity improvement projects must meet one or a combination of the following functional requirements:

- **Prevention from Information security incidents:** Use Password Safe to prevent attacks and incidents caused by bad passwords and their improper management.
- **Information security incident detection:** All actions in Password Safe are documented and can be traced in an audit-proof manner afterwards.
- **Mitigation of information security incidents:** Through additional security mechanisms such as 2FA, security levels, multi-eye principle, etc., potential incidents are mitigated in advance.
- **Increase and maintain awareness of information security incidents or the importance of IT/cybersecurity:** With features such as password policy compliance, password quality display, etc., employees are instructed to be more aware of the use of passwords.

Why Password Safe?

Experience

MATESO has focused on professional enterprise password management since **2006**. Over **20 of the top 40 DAX companies** and more than **10,000 users** already rely on Password Safe for password protection.

Comprehensive protection

With the influence of over **20 years of market experience**, the solution is holistically tailored to the individual security requirements and needs of companies. All passwords are protected holistically throughout the **password lifecycle** - from creation to archiving.

Made in Germany

As a member of the TeleTrust initiative **„IT-Security Made in Germany“**, MATESO stands for trustworthy IT security solutions that meet the requirements of German data protection law, can be used in **compliance with the DSGVO** and do not contain any hidden accesses.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE