MULTI-TALENTS IN EVERYDAY HOSPITAL LIFE

Modern authentication solutions for healthcare

The security of people and data must always come first, especially in hospitals, despite time pressures. A modern system that regulates user authentication and access to sensitive areas—as well as access to medicines, medical equipment and information requiring protection—can significantly improve the level of security. But that's not all: it can also simplify processes, speed them up and make them more transparent. This increases efficiency and thus reduces costs. At the same time, it increases convenience for staff and patients. In order to make the solution sustainable and future-proof, hospital operators need to consider important points during implementation.

Personal health data is among the most sensitive information. The patient file must therefore be protected accordingly, and access to it must be restricted to a select group of people, consisting of the treating physicians and nursing staff. In the event of data protection violations, there is not only the threat of severe fines but also a loss of reputation for the hospital. At the same time, however, the information must be available quickly and easily in an emergency. The same applies to access to medicines or medical equipment, which also only belong in authorized hands. And access to sensitive areas such as operating rooms, neonatal or intensive care units must also be reliably restricted to the circle of authorized persons. On the other hand, it is important that the hospital premises are easily accessible not only to doctors, nursing staff, cleaners and administrative staff, but also to patients and visitors. Reconciling all these requirements can be an enormous challenge for hospital operators.

Smooth authentication with RFID and mobile technologies

A secure, fast, and convenient access control solution is needed to manage the balancing act between protection and smooth day-to-day hospital operations. Modern authentication solutions based on RFID or digital credentials have proven to be particularly efficient and reliable.

A simple, inexpensive and proven option for implementing user authentication and access control is an RFID-enabled employee ID card, which is already used in many cases for staff identity proofing. The identification process is automatic once the card is held up to a reader. This gives hospital employees immediate access to all facilities, areas, data and equipment for which they have authorization. Depending on the employee's area of responsibility and qualifications, the authorizations can be easily and individually adjusted. This has the advantage of significantly speeding up the numerous authentication processes that staff have to go through in the course of a shift, which increases efficiency in the day-to-day running of the clinic and relieves the burden on doctors and medical staff. They can thus invest the time gained in treating patients. Clinic operators benefit not only from lower costs due to the improved processes, but also in terms of their image as an employer.

In addition to the classic employee ID card, it is also possible to use digital credentials based on NFC (Near Field Communication) or BLE (Bluetooth® Low Energy), with which the majority of all mobile devices such as smartphones or tablets are equipped. This type of authentication is particularly appropriate for use by patients, who also benefit from a modern authentication and access control system. For example, they have the option of conveniently using their cell phones to pay in the cafeteria or log in to use communication and entertainment systems. The use of wearables, for example in the form of wristbands, is also possible.

Authorizations for patients and staff can be easily managed centrally by hospital IT staff. If employees change locations within a hospital group, for example, the authorizations can be changed accordingly with little effort. When patients are discharged, the authorizations are simply deleted.

A system with many application possibilities

A uniform system for user authentication offers a wide range of possible applications. One example is multimedia terminals in patient rooms, which are equipped with a multifrequency reader and can be used easily by both parties. While staff members identify themselves with their ID cards, patients can use their smartphones, for example. Clinic staff can thus access digital patient data via the device at the patient's bedside, while patients can conveniently use the same terminal later to access entertainment and services.

A uniform system also opens up numerous other possibilities. The spectrum ranges from employee time recording and cafeteria payment, to employee and visitor access to designated parking spaces, to the use of employee lockers or single sign-on for the hospital network. Even the secure printing of sensitive documents such as lab results, diagnoses or medication prescriptions can be achieved using the same authentication solution. This not only increases security but also saves time, as PINs or passwords no longer have to be entered at the printer. Another advantage is that the authentication solution can also be integrated into elevators in the form of an access control system. Employees and patients simply hold their ID card or smartphone up to the reader before selecting a floor and can thus access only the floors that have been unlocked for them.

Tips for successful implementation

To ensure that the introduction of such a comprehensive solution is a success, particular attention must be paid to the following aspects during implementation.

Flexibility through universal readers
A variety of card technologies are available on the international market, each with its own data formats, communication frequencies and security functions. Especially for clinics with multiple locations, employee badges with different technologies may be in use. However, most readers are only capable of reading a few card technologies. A solution is offered by multifrequency readers that are compatible with up to 60 transponder technologies commonly used worldwide. The universal devices, which solution provider Elatec has in its portfolio, for example, use both RFID and NFC or BLE technologies for authentication and access. This makes it possible to integrate smartphones or wristbands into the system, providing the greatest possible flexibility.

Security - a question of the overall system
Authentication and access control systems serve to protect people, buildings, physical assets and data. To ensure this, the systems themselves must be secured against manipulation. This is because security gaps pose an enormous risk—especially in the age of digital transformation.

When selecting an RFID reader as a central component of an access solution, care must be taken to ensure that it supports the credentials and encryption algorithms appropriate for the application's security level. The readers used must be equipped against physical manipulation as well as hacker attacks. However, to effectively and holistically secure an RFID-based authentication solution, it is not enough to look at the reader alone. It is necessary to include the entire system in the hospital's security concepts. This is a complex process which, in brief, proceeds as follows: based on a real existing or feared threat scenario, a protection concept is developed, which forms the basis for the implementation of the specific protection. This can be achieved by a technical element as well as a procedure or process. In any case, the following applies: security must always be related to the overall system.

Ready for the future thanks to central remote maintenance
Requirements and IT infrastructures change over time and make adjustments necessary. Only with a flexible system that provides for optimizations, adaptations and upgrades will clinics be on the safe side in the future. This is because a system often comprises hundreds of readers, which are frequently distributed over a wide area or even different locations. As a rule, updates would have to be laboriously applied by a technician to each individual device directly onsite. If remote updates or upgrades are possible, on the other hand, all installed readers can be updated easily and quickly from a central system, regardless of their location—a decisive advantage.

Practical example: Simple and secure authentication for disinfection chambers

According to the Robert Koch Institute (RKI), around 18 million people are treated as inpatients in German hospitals and other healthcare facilities every year. Hygiene protocols are used to keep the risk of infection for patients and staff as low as possible. Sterilization and disinfection measures make a major contribution in this context—whether for surgical instruments, surfaces, equipment, beds or patient transport chairs. However, the highly technical equipment required for this must be used properly to produce the desired result. Moreover, handling the equipment is not without risk—for example, UV radiation used for disinfection and sterilization can cause damage to eyes and skin, among other things, if used improperly. Hospitals must therefore ensure that their staff are only authorized to operate the equipment after successfully completing training. User authentication by means of RFID, which manufacturers can integrate into their devices, is suitable for this purpose.

Finding the right reader for such an application often proves challenging for vendors because the list of requirements is long. For one, the reader must support the security and functionality needs of a vendor's hospital customers. It should also be able to handle multiple RFID card technologies. This aspect is especially important if different technologies are already in use in a hospital or a hospital group with multiple locations. In addition to technology, however, the reader's aesthetics also count in the hospital environment: the device should fit seamlessly into the appearance of a clean, efficient hospital environment.

The example of UV-Concepts shows how the requirements in terms of security, flexibility and appearance can be solved. The American company develops and manufactures innovative, non-contact disinfection solutions. The centerpiece of the UV-Concepts portfolio is a UV-C chamber that irradiates its contents with ultraviolet UV-C waves to kill germs safely. This means that even large items such as wheelchairs can be disinfected easily and reliably. To protect the chamber against unauthorized use by untrained employees, UV-Concepts relies on Elatec's TWN4 Palon Compact Panel reader. The reader features a robust yet flexible software architecture combined with a panel display suitable for high-end devices that is visually compelling. It can also be configured for more than 60 RFID card transponder technologies. This is a decisive advantage for UV-Concepts, as the reader enables the company to optimally serve those customers who use multiple technologies.

Author

Burhan Gündüz, Vice President Secure Printing EMEA & Japan at ELATEC GmbH

In cooperattion with

ident