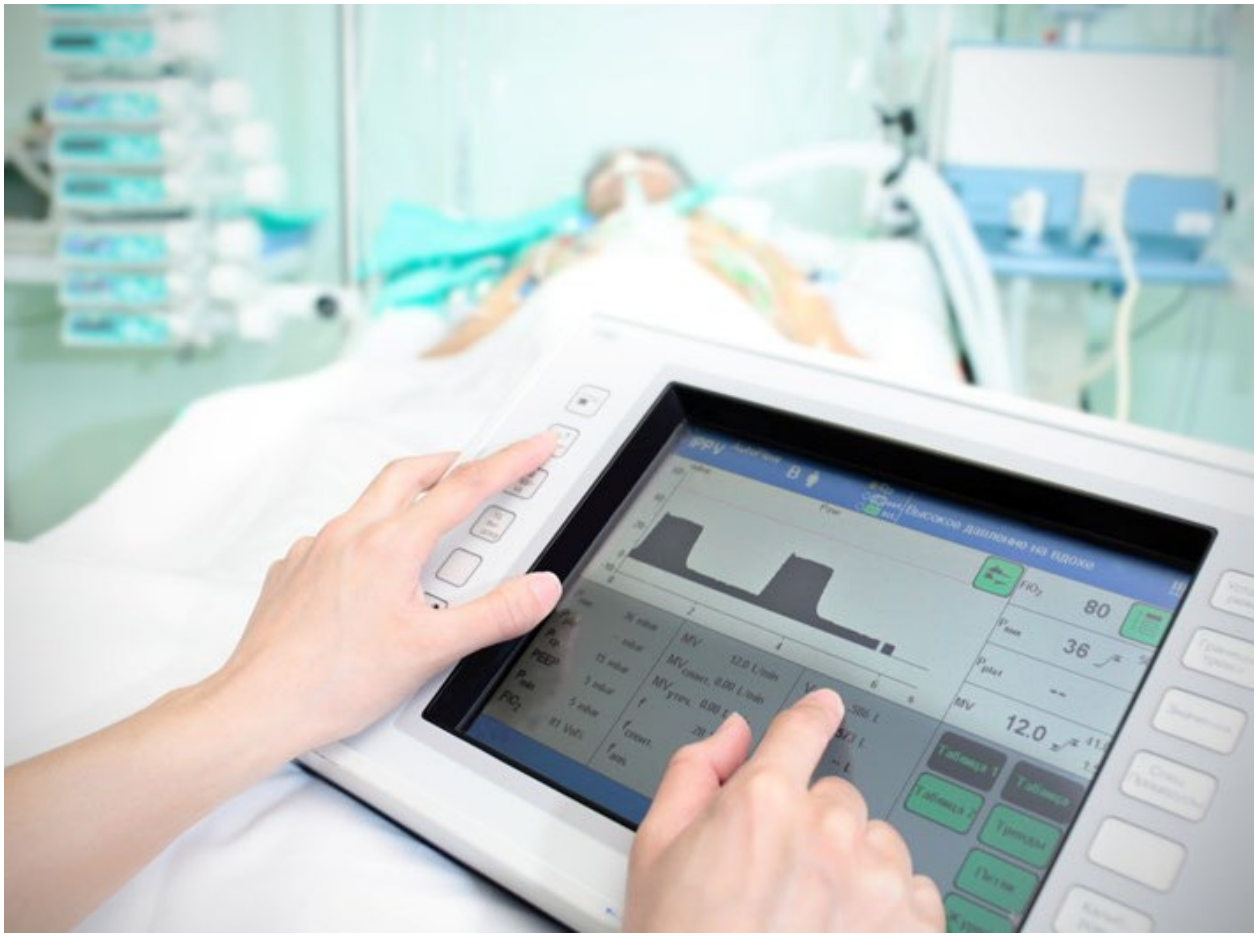
ELATEC
RFID Systems

INCREASE EFFICIENCY AND COMFORT

Modern authentication solutions for clinics



Even though things often have to move quickly in the day-to-day running of a clinic, it is important to maintain high security standards despite the time pressure. With a modern system that regulates user authentication as well as access, sensitive information and areas be effectively protected from unauthorized persons. It also enables simple, fast and transparent processes and increases convenience for staff and patients. To ensure that the solution is sustainable and future-proof, hospital operators must consider important points during implementation.

Personal health data belongs to the category of particularly sensitive information. Therefore, only the attending physicians and nursing staff may be allowed to look at the patient file. In the event of violations, there is not only the threat of severe fines, but also a loss of reputation for the hospital. On the other hand, the information must be available quickly—for example, when an emergency occurs. 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 and neonatal or intensive care units must also be reliably restricted to the circle of authorized persons. On the other hand, it is necessary to ensure that the hospital premises are easily accessible not only to doctors, nursing staff, administrative employees and cleaning staff, but also to patients and visitors. In terms of security, therefore, those responsible in clinics face a number of challenges.

Smooth authentication with RFID and mobile technologies

To manage this balancing act between protection and smooth access and entry in the hospital environment, responsible parties can rely on technical support. 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 a badge equipped with an RFID chip—which most employees already carry in the form of an ID card. When the card is held up to a reader, the identification process is automatic. Hospital employees have instant access to all areas and facilities, data and equipment for which they are authorized. This significantly speeds up the numerous authentication processes required of staff during the course of a shift. It also increases efficiency in the day-to-day running of the clinic and leaves more time for patient treatment.

The system can also be used to create transparency with regard to the efficiency of processes in the clinic. In this way, optimization potential can be identified.

Currently, the classic ID card is still the identification medium of choice for employees. For patients and visitors, on the other hand, the use of digital credentials on smartphones is already an option. For this purpose, the technologies NFC (Near Field Communication) or BLE (Bluetooth® Low Energy) are used, with which a majority of all mobile devices such as smartphones are equipped. In this way, patients benefit from a modern access control system in that they can, for example, use their cell phone to conveniently pay in the cafeteria or register to use communication and entertainment systems.

Authorizations for patients and staff can be 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, their authorizations are simply deleted.

One solution, many applications

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 reader and can be used easily by both parties. Both staff and patients simply identify themselves with an ID card or their smartphone. Hospital staff thus access digital patient data via the device at the patient's bedside, while patients conveniently use the same terminal later to access entertainment and services. A unified system also opens up numerous other possibilities, ranging from time recording to paying in the cafeteria, access to parking spaces, use of employee lockers, and one-time registration for the hospital network.

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 multi-frequency readers that are compatible with up to 60 transponder technologies commonly used worldwide. The universal devices, which the solution provider Elatec has in its portfolio, for example, use both RFID and the NFC or BLE technologies for authentication and access. This makes it possible to integrate mobile end devices into the system, providing the greatest possible flexibility.

Total system security

Authentication and access control systems serve to protect people, buildings, equipment 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 on site. If remote updates or upgrades are possible, on the other hand, all installed readers can be updated easily and quickly from a central location, regardless of their location—a decisive advantage.

Author

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

ELATEC GmbH

Zeppelinstr. 1

82178 Puchheim, Germany, Phone: +49 89 552 9961 0,E-mail: info-rfid@elatec.com

In cooperattion with

Health&Care Management