

Authentifizierungslösungen

Mehr Effizienz und Komfort

Im Klinikalltag gilt es, die hohen Sicherheitsstandards trotz des Zeitdrucks einzuhalten. Mit einem System, das Benutzerauthentifizierung sowie Zutritt und Zugang regelt, sollen sensible Informationen und Bereiche effektiv vor unbefugten Personen geschützt werden. Was es zu beachten gilt.

Die persönlichen Gesundheitsdaten zählen zur Kategorie der besonders sensiblen Informationen. Der Blick in die Patientenakte darf daher nur der behandelnden Ärzteschaft und dem Pflegepersonal erlaubt sein. Bei Verstößen drohen nicht nur empfindliche Geldbußen, sondern auch ein Reputationsverlust für das Krankenhaus. Andererseits müssen die Informationen schnell verfügbar sein – beispielsweise beim Eintreten eines Notfalls. Gleiches gilt für den Zugang zu Medikamenten oder medizinischen Geräten, die ebenfalls nur in autorisierte Hände gehören. Und auch der Zutritt zu sensiblen Bereichen wie OP-Räumen, Neugeborenen- oder Intensivstationen muss zuverlässig auf den Kreis berechtigter Personen beschränkt werden. Außerdem ist es erforderlich, dass das Klinikgelände nicht nur für Ärzteschaft, Pflegepersonal, Verwaltungsangestellte und Reinigungskräfte, sondern auch für Patientinnen und Patienten sowie Besuchende einfach zugänglich ist. In puncto Sicherheit stehen die Verantwortlichen in Kliniken also vor einer Reihe von Herausforderungen.

RFID und mobile Technologien

Um diesen Spagat zwischen Schutz und einem reibungslosen Zutritt und Zugang im Klinikumfeld zu bewältigen, können Verantwortliche auf technische Unterstützung setzen. Moderne Authentifizierungslösungen auf Basis von RFID oder digitalen Berechtigungsnachweisen haben sich als besonders effizient und zuverlässig erwiesen.



Moderne Authentifizierungslösungen regeln Zugang und Zutritt zu sensiblen Informationen und Bereichen.

Eine einfache, günstige und bewährte Option zur Implementierung von Benutzerauthentifizierung und Zugangskontrolle ist ein Ausweis, der mit einem RFID-Chip ausgestattet ist – und den die meisten Mitarbeiter in Form einer ID-Karte bereits bei sich tragen. Wird die Karte an ein Lesegerät gehalten, erfolgt der Identifizierungsprozess automatisch. So wird den Klinikangestellten umgehend Zutritt zu allen Bereichen und Zugriff auf alle Einrichtungen, Daten und Geräte gewährt, für die sie autorisiert sind. Die zahlreichen erforderlichen Authentifizierungsprozesse, die das Personal im Laufe einer Schicht durchführen muss, können so erheblich beschleunigt werden. Dies trägt dazu bei, die Effizienz im Klinikalltag zu steigern und bringt mehr Zeit für die Behandlung der Patientinnen und Patienten.

Derzeit ist für die Mitarbeitenden der klassische Ausweis in der Regel noch das Identifikationsmedium der Wahl. Für die zu behandelnden Menschen hingegen stellt der Einsatz von digitalen Berechtigungsnach-

weisen auf dem Smartphone bereits eine Option dar. Hierfür lassen sich die Technologien NFC (Near Field Communication) oder BLE (Bluetooth Low Energy) nutzen, mit denen ein Großteil aller mobilen Endgeräte wie Smartphones ausgestattet sind. Patientinnen und Patienten profitieren von einem modernen Zutritts- und Zugangskontrollsystem, indem sie z.B. mit ihrem Handy komfortabel in der Cafeteria zahlen oder sich für die Nutzung von Kommunikations- und Entertainmentsystemen anmelden können. Die Berechtigungen können durch die Klinik-IT zentral verwaltet werden. Wechseln Angestellte beispielsweise innerhalb eines Klinikverbundes den Standort, lassen sich die Berechtigungen mit geringem Aufwand entsprechend ändern. Bei der Entlassung werden die Berechtigungen der Patientinnen sowie Patienten einfach gelöscht.

Lösung für viele Anwendungen

Ein einheitliches System für die Benutzerauthentifizierung bietet

eine Vielzahl von Möglichkeiten. Ein Beispiel sind Multimediaterminals in den Patientenzimmern, die mit einem Lesegerät ausgerüstet sind und problemlos von beiden Parteien genutzt werden können. Sowohl das Personal als auch die Patientinnen und Patienten identifizieren sich mit einer Ausweiskarte oder ihrem Smartphone. Das Klinikpersonal kann so über das Gerät am Bett der zu behandelnden Person auf die digitalen Patientendaten zugreifen. Die Patientinnen und Patienten können dasselbe Terminal später nutzen, um Zugang zu Unterhaltungs- und Serviceangeboten zu erhalten. Das einheitliche System bietet noch weitere Vorteile wie:

- Zeiterfassung,
- Zahlen in der Kantine,
- Zufahrt zu Parkplätzen,
- Nutzung von Spinden der Mitarbeitenden sowie Einmalanmeldung im Krankenhausnetzwerk.

Erfolgreiche Implementierung

Für den Erfolg bei der Einführung sollte Folgendes beachtet werden:

- Flexibilität: Am internationalen Markt sind eine Vielzahl von Kartentechnologien mit jeweils eigenen Datenformaten, Kommunikationsfrequenzen und Sicherheitsfunktionen verfügbar. Gerade für Kliniken

mit mehreren Standorten gilt, dass Ausweise der Mitarbeitenden mit unterschiedlichen Technologien im Einsatz sein können. Hier bieten sich Multifrequenz-Lesegeräte an, die mit bis zu 60 weltweit gängigen Transpondertechnologien kompatibel sind. Die universellen Geräte, die z.B. der Lösungsanbieter Elatec im Portfolio hat, nutzen für Authentifizierung und Zugang sowohl RFID als auch die Technologien NFC oder BLE. Damit ist es möglich, mobile Endgeräte ins System einzubinden.

- Sicherheit: Zutritts- und Zugangskontrollsysteme dienen zum Schutz von Menschen, Gebäuden, Einrichtungen und Daten. Damit sie dies gewährleisten können, müssen die Systeme selbst gegen Manipulationen abgesichert werden. Denn Sicherheitslücken stellen – speziell im Zeitalter der digitalen Transformation – ein enormes Risiko dar. Bei der Auswahl eines RFID-Lesegeräts als zentralem Bestandteil einer Zutritts- und Zugangslösung ist darauf zu achten, dass es die für die Sicherheitsstufe der Anwendung geeigneten Anmeldedaten und Verschlüsselungsalgorithmen unterstützt. Die verwendeten Lesegeräte müssen gegen physische Manipulationen ebenso wie gegen Hackerangriffe

gerüstet sein. Es ist notwendig, das komplette System in die Sicherheitskonzepte der Klinik einzubeziehen. Dies sollte wie folgt ablaufen: Auf Basis eines real vorhandenen oder befürchteten Bedrohungsszenarios wird ein Schutzkonzept entwickelt, das die Grundlage für die Umsetzung des spezifischen Schutzes bildet. Dieser kann durch ein technisches Element, ein Verfahren oder einen Prozess erreicht werden. Stets gilt: Die Sicherheit muss immer auf das Gesamtsystem bezogen sein.

- Zentrale Fernwartung: Anforderungen und IT-Infrastrukturen verändern sich im Laufe der Zeit und machen Anpassungen erforderlich. Es braucht ein flexibles System, das Optimierungen, Adaptionen und Upgrades vorsieht. Ein System umfasst oft hunderte Lesegeräte, die häufig über ein weitläufiges Gelände oder verschiedene Standorte verteilt sind. In der Regel müssten Updates aufwendig auf jedes einzelne Gerät vor Ort aufgespielt werden. Sind Remote-Updates oder -Upgrades möglich, können alle installierten Lesegeräte unabhängig vom Standort von zentraler Stelle aktualisiert werden.

Burhan Gündüz,

Kontakt: B.Guenduez@elatec.com

Effektive Fortbildungen - organisiert im Handumdrehen

Mit der E-Learning-Lösung von Relias kein Problem!

Die Relias Lernplattform nimmt Ihnen zeitaufwendige Tätigkeiten ab. Unsere abwechslungsreich gestalteten Online-Kurse werden automatisch zugewiesen und stehen jederzeit zum Lernen bereit. Das Berichtswesen liefert zuverlässig alle benötigten Informationen.

Sie möchten mehr wissen? Kontaktieren Sie uns!

Wir zeigen Ihnen gern unsere Lösungen.



Erleben Sie
unsere Lösungen auf einer Messe
oder in einem Live-Webinar:
www.relias.de/veranstaltungen

RELIAS

Ihr Partner für E-Learning im Gesundheitswesen
Pflichtfortbildungen, Expertenstandards und
Fachfortbildungen online schulen
0800 72 34 785 | kontakt@relias.de | www.relias.de