Auszug aus März 2025 | Ausgabe 3
52. Jahrgang
ISSN 1619-4772
KZ B 1494

KTM

Krankenhaus

TECHNIK+MANAGEMENT

Die Fachzeitschrift für den HealthCare-Markt

Titelstory
Händehygiene-Compliance gestärkt

Special
Hygiene

Themen

Simulationstraining:
Teamwork fördern

Umweltcoaches:
Nachhaltigkeit auf der Spur

Hygienemängel
sind keine Lappalie

medhochzwei

fbmt fachverband biomedizinische technik
DGTelemed
Offizielles Organ des fbmt und der DGTelemed

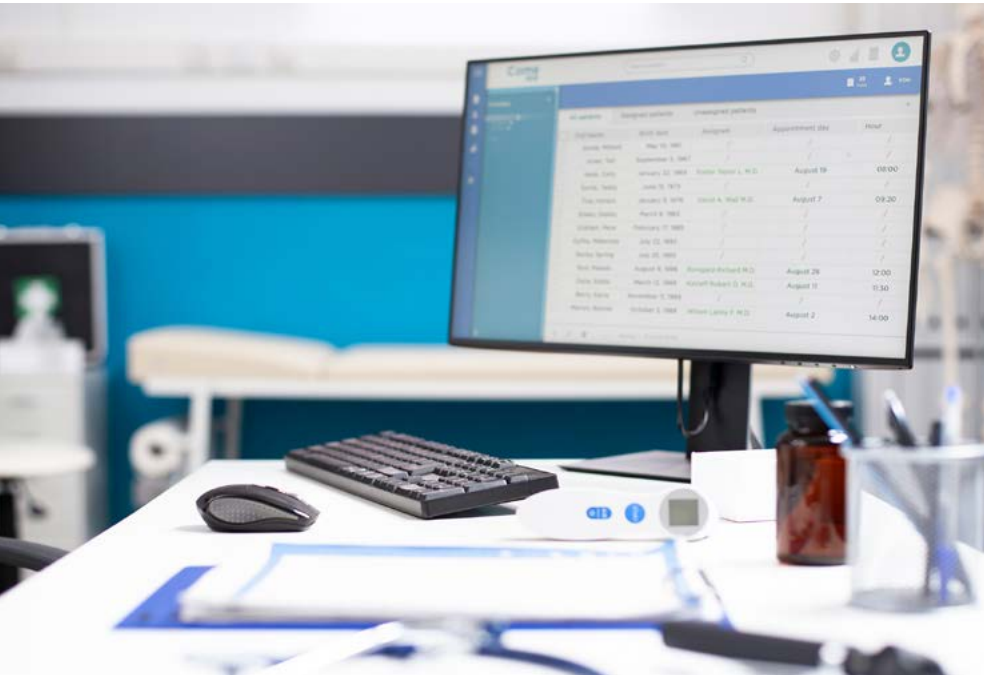
Mit berührungsloser Authentifizierung Effizienz und Sicherheit in Kliniken und Arztpraxen erhöhen

Daten schützen, Personal entlasten

Der Schutz sensibler Patientendaten und die Entlastung des medizinischen Personals sind zentrale Herausforderungen, gerade vor dem Hintergrund der Einführung der elektronischen Patientenakte (ePA). Das gilt insbesondere in sensiblen Bereichen wie Behandlungszimmern, in denen Patientendaten auf Monitoren sichtbar und PCs oft unbeaufsichtigt sind. Wie lässt sich Datenschutz gewährleisten, ohne die Arbeitsabläufe zu behindern? Berührungslose Authentifizierung mit Bluetooth-Token bietet hier eine Lösung. Sie optimiert Arbeitsabläufe, erhöht die Sicherheit und entlastet das Personal von zeitaufwändigen manuellen Passworteingaben.

Die Datenschutz-Grundverordnung (DSGVO) gibt in Artikel 32 unmissverständlich vor, dass Krankenhäuser und Kliniken geeignete technische und organisatorische Maßnahmen (TOM) ergreifen müssen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Dazu gehört, dass Monitore so positioniert werden, dass unbefugte Einblicke verhindert werden, und dass Computer automatisch gesperrt werden, sobald sie unbeaufsichtigt sind. Doch die praktische Umsetzung der Vorgaben erweist sich in vielen Kliniken als schwierig. Häufig werden Arbeitsplätze unter Zeitdruck und ungesperrt verlassen, und die manuelle Passworteingabe für die Wiederanmeldung ist nicht nur zeitaufwendig, sondern auch fehleranfällig.

Untersuchungen in einem US-amerikanischen Krankenhaus haben gezeigt, dass in einer Abteilung mit 20 Mitarbeitern bis zu 120 Anmeldungen pro Stunde durchgeführt wurden. Das Beispiel verdeutlicht, wie sehr manuelle Authentifizierungsprozesse die Effizienz beeinträchtigen und gleichzeitig die Gefahr erhöhen, dass Mitarbeiter aus Zeitdruck Sicherheitsmaßnahmen umgehen – sei es durch das Aufschreiben von Passwörtern auf Notizzetteln oder das Teilen von Zugangsdaten. Hier setzt eine moderne Lösung an, die Sicherheit und Benutzerfreundlichkeit vereint: zentral verwaltbare Bluetooth-Token.



Zum Schutz sensibler Patientendaten müssen Monitore so positioniert sein, dass Unbefugte keinen Einblick erhalten, und unbeaufsichtigte PCs automatisch gesperrt werden. Doch die praktische Umsetzung erweist sich oft als schwierig. Häufig werden Arbeitsplätze unter Zeitdruck ungesperrt verlassen. Bild: DC Studio/stock.adobe.com

Authentifizierung berührungslos per Bluetooth-Token

Bluetooth-Token sind kleine, zentral verwaltbare Hardware-Geräte, die als digitaler Schlüssel fungieren. Jeder Token ist eindeutig einem Nutzer zugeordnet und kommuniziert automatisch mit den Computern im Kliniknetzwerk, sobald dieser in die Nähe eines Arbeitsplatzes kommt. Ihm wird individueller Zugang gewährt, ohne dass der Nutzer Passwörter eingeben muss. Entfernt er sich vom Arbeitsplatz, sperrt der Computer entweder automatisch den Bildschirm oder meldet den Nutzer ab – je nach Konfiguration. So stellt der Schutzmechanismus sicher, dass sensible Daten niemals unbeaufsichtigt zugänglich sind.

Technisch basiert die Lösung auf der verschlüsselten Übertragung von Authentifizierungsdaten via Bluetooth und auf einer zentralen Verwaltungssoftware, die den gesamten Prozess überwacht. Die Plattform ermöglicht IT-Administratoren die einfache Konfiguration und Überwachung der Token sowie die Anpassung von Zugriffsrechten in Echtzeit. Die Integration in bestehende IT-Systeme und deren Verzeichnisdienste wie das Active Directory erfolgt dabei nahtlos.

Mehr Effizienz im Klinikalltag

Die Vorteile der Technologie für den Klinikalltag sind enorm. Besonders in komplexen Umgebungen und hochdynamischen Situationen, wie etwa in der Notaufnahme, zählt jede Sekunde. Berührungslose Authentifizierung ermöglicht es dem medizinischen Personal, sich auf die Patientenversorgung zu konzentrieren, anstatt technische Hürden zu überwinden.

Darüber hinaus reduziert die Technologie menschliche Fehler, die in Stresssituationen auftreten können. Vergessene Passwörter, unsichere Notizen oder das versehentliche Offenlassen eines Arbeitsplatzes gehören mit Bluetooth-Token der Vergangenheit an. Und auch Patienten profitieren von den Verbesse-

rungen, da die gewonnene Zeit direkt in ihre Versorgung fließen kann.

Besserer Datenschutz durch geringe Implementierungshürden

Die Einführung der Technologie ist unkompliziert und stellt an Krankenhäuser überschaubare Anforderungen. In den meisten Fällen sind keine umfangreichen Anpassungen der bestehenden IT-Infrastruktur notwendig. Arbeitsstationen können mit Bluetooth-Empfängern nachgerüstet werden, die zentrale Verwaltungslösung wird einfach in das bestehende Kliniknetzwerk eingebunden. Die Kosten beschränken sich auf die Anschaffung der Hardware-Token und der Managementsoftware sowie auf Schulungen, die dank intuitiver Anwendung nur wenig Zeit in Anspruch nehmen.
Die Implementierung ist auch aus rechtlicher Sicht eine Erleichterung: Die Technologie unterstützt die Einhaltung der DSGVO, indem sie sensible Daten schützt und detaillierte Zugriffsprotokolle bereitstellt. Sie erleichtert die Dokumentation

Manuelle Authentifizierung erhöht die Gefahr, dass aus Zeitdruck Sicherheitsmaßnahmen umgangen werden. Hier setzt eine moderne Lösung mit Bluetooth-Token an. Sobald der Mitarbeiter in die Nähe eines Arbeitsplatzes kommt, wird ihm Zugang gewährt, ohne dass er Passwörter eingeben muss. Bild: Untethered Labs

Besonders in komplexen und hektischen Situationen, wie etwa in der Notaufnahme, ermöglicht berührungslose Authentifizierung dem medizinischen Personal, sich auf das Wesentliche zu konzentrieren: die Patientenversorgung.

Bild: Dennis M. Swanson/stock.adobe.com

und das Reporting im Rahmen von Audits erheblich.

Effiziente Verwaltung und Kontrolle für IT-Administratoren

Zentral verwaltbare Bluetooth-Token bieten IT-Administratoren praktische Vorteile bei der Verwaltung von Zugriffsrechten und der Sicherheit von Computersystemen. Die Technologie reduziert den Aufwand für die Passwortverwaltung erheblich, da Passwörter nicht mehr manuell zurückgesetzt oder verteilt werden müssen. Über die zentrale Lösung können Zugriffsrechte flexibel gesteuert und angepasst werden – etwa, dass Nutzer nur auf bestimmte Computer oder mit begrenzten Rechten Zugriff erhalten. Alle Anmelde- und Abmeldeaktivitäten können in Echtzeit protokolliert und ausgewertet werden. Das schafft Transparenz und erleichtert die Einhaltung von Datenschutzanforderungen. Darüber hinaus ermöglicht die zentrale Steuerung schnelles Handeln, zum Beispiel beim Verlust eines Tokens – ohne die laufenden Arbeitsprozesse zu beeinträchtigen. Mit ihren Funktionen ermöglicht es die Lösung, die Anforderungen an Sicherheit und Kontrolle effizient zu erfüllen.

‚Halberd Token' des Herstellers GateKeeper bietet zusätzliche Sicherheitsmechanismen für den Verlust oder Diebstahl eines Token. Das System lässt sich so konfigurieren, dass der Anwender sich nicht ausschließlich per Annäherung einloggen kann, sondern zusätzlich eine PIN oder einen Passcode eingeben muss.

Sicherheit und Effizienz im Einklang

Die berührungslose Authentifizierung mittels Bluetooth-Token bietet eine zukunftsweisende Lösung für die Herausforderungen des digitalen Gesundheitswesens. Sie vereint höchste Sicherheitsstandards mit einer intuitiven Benutzererfahrung und trägt dazu bei, die Arbeitsabläufe in Kliniken und Arztpraxen nachhaltig zu verbessern. Die einfache Implementierung und die erheblichen Vorteile machen die Technologie zu einer wichtigen Investition in die Zukunft – für Patienten, Mitarbeiter und das Klinikmanagement.

Robert Korherr

Kontakt:

ProSoft GmbH
Robert Korherr (CEO)
Bürgermeister-Graf-Ring 10
82538 Geretsried
Tel.: +49 8171 405-0
info@prosoft.de
www.prosoft.de

Vorteile der Bluetooth-Token-Technologie:

- Zeitersparnis durch automatisierte An- und Abmeldung: manuelle Passworteingaben entfallen, Arbeitsabläufe werden beschleunigt
- Erhöhte Datensicherheit durch automatische Sperrfunktion: Unbeaufsichtigte Arbeitsplätze werden automatisch gesperrt, angemeldete Anwender abgemeldet. Sensible Daten sind so permanent vor unbefugter Einsicht geschützt.
- Reduzierung menschlicher Fehler: kein Vergessen oder Weitergeben von Passwörtern, weniger Sicherheitsrisiken
- Nahtlose Integration in bestehende IT-Systeme: kompatibel mit bestehender Klinik- und Praxissoftware
- Einhaltung von Datenschutzstandards (DSGVO): Audits und die Einhaltung gesetzlicher Vorgaben werden erleichtert
- Verbesserte Effizienz und Patientenversorgung: Mitarbeiter gewinnen Zeit für die direkte Patientenversorgung.