FACTS & FEATURES

IT-Sicherheit in Krankenhäusern

Auch, wenn es schnell gehen muss.

Chance auf geförderte Maßnahmen nutzen

Jedes Krankenhaus wird kurzfristig im Rahmen des KHZG (Krankenauszukunftsgesetzes) geförderte Maßnahmen u.a. im Bereich der IT-Sicherheit umsetzen müssen.

Wir sind Ihr zertifizierter Partner für IT-Sicherheit und tragen dazu bei, dass …

… PC-Arbeitsplätze nicht mehr unbeaufsichtigt offen stehen

… vertrauliche Daten verschlüsselt und dennoch komfortabel nutzbar bleiben

… Daten auch beim Versenden außer Haus vertraulich bleiben

Technische Sofortlösungen für Krankenhäuser

Gemeinsam mit unseren Kunden im medizinischen Bereich haben wir technische Sofortlösungen entwickelt, welche vertrauliche Daten zuverlässig schützen, den Mitarbeitern eine schnelle und einfache An- und Abmeldung an den PCs ermöglichen und Ärzte und Krankenhauspersonal vor ungewollten Datenschutzvergehen bewahrt.

Zertifizierter Partner für IT-Sicherheitsmaßnahmen im Rahmen des KHZG

Das können wir für Sie tun

- ✓ 360° Schutz für Patienten- und Mitarbeiterdaten
- ✓ Bequeme An- und Abmeldung an Arbeitsplatz-PC (auch an Stations-PCs mit häufigem Nutzerwechsel)
- ✓ Protokollierung aller Anmeldungen und Zuordnung zum Nutzerprofil
- ✓ Sicherer und schneller Versand auch großer Dateien
- ✓ Schutz der Ärzte und des Krankenhauspersonals vor ungewollten Datenschutzvergehen

Unser Versprechen als Hersteller

Alle Lösungen aus unserem Haus sind aufgrund von konkreten Anforderungen und Bedürfnissen aus der Praxis entstanden. Viele individuelle Konfigurationsmöglichkeiten bringen die Lösungen daher schon mit. Als Hersteller entwickeln wir jedoch auch gern gemeinsam mit Ihnen Anpassungen, die Ihre spezifischen Anforderungen bestmöglich erfüllen.

Kontakt

digitronic®
computersysteme gmbh
Oberfrohnaer Str. 62
09117 Chemnitz

+49 371 81539 0
vertrieb@digitronic.net
www.digitronic.net

https://www.digitronic.net/gesundheitsbereich

IT-Sicherheit in Krankenhäusern

Auch, wenn es schnell gehen muss.

3 Lösungen für umfassenden Schutz

Schnelle und sichere An- und Abmeldung an PCs mittels 2-Faktor-Authentifizierung

SmartLogon™ ist eine 2-Faktor-Authentifizierung, welche die normale Windows-Anmeldung für Ihre Mitarbeiter ersetzt. Lange, komplizierte Passwörter oder offen stehende PCs waren gestern. Die Lösung lässt sich kurzfristig an beliebig vielen Arbeitsplätzen implementieren und wenn nötig auf Ihre individuellen Anforderungen anpassen.

Praxisszenario (Beispiel)*:

- PC-Anmeldung mittels Authentifizierungs-Merkmal (Token) und kurzer PIN

- Als Token eignen sich Smartcards, USB- oder Bluetooth-Token und sogar Smartphones

- Protokollierung aller Anmeldungen und Zuordnung zum jeweiligen Nutzerprofil

  Öffnen individueller Anwendungen entsprechend des Profils

  Praktisch für stark frequentierte Stations-PCs mit schnellen Nutzerwechseln

- Automatische Abmeldung bei Entfernen des Tokens oder Verlassen des Geräts

*Das genannte Praxisszenario ist nur ein Beispiel. Workflow und Funktionen können flexibel auf Ihre Anforderungen angepasst werden.

IT-Sicherheit in Krankenhäusern

Auch, wenn es schnell gehen muss.

3 Lösungen für umfassenden Schutz

Sicherer Transfer auch großer Emails mit vertraulichem Inhalt

Vor allem im medizinischen Bereich, wo vertrauliche Informationen von A nach B gesendet werden müssen, sollte sichergestellt werden, dass sensible Daten weder beim Abspeichern noch während der Übertragung abgefangen und Dritten zugänglich gemacht werden können.

Um genau diesen 360° Schutz für „Data at Rest" und „Data in Transit" zu gewährleisten, haben wir mit der Cryptshare AG eine Technologie-Partnerschaft geschlossen. Cryptshare stellt mit ihrer Email-Verschlüsselung sicher, dass Informationen und Dateien während des Transfers gegen Angriffe Dritter zuverlässig geschützt sind. Auch sehr große Dateien mit Anhang können über diesen sicheren Weg schnell und zuverlässig gesendet und empfangen werden.

Elektronische Patientendaten sicher im digitalen Tresor verwahren

Unsere Verschlüsselungslösung HiCrypt™ schützt sämtliche Daten vor und nach dem Versand, indem sie diese auf Netzlaufwerken kryptografisch codiert ablegt und so in einem digitalen Tresor sicher verwahrt.

Die Software ist in wenigen Minuten installiert, läuft geräuschlos im Hintergrund und lässt sich intuitiv bedienen. Die Schlüsselverwaltung wird nur von Personen durchgeführt, die ausschließlich für die Vertraulichkeit der Dateninhalte verantwortlich sind (z.B. Qualitätsbeauftragter). Administratoren können zwar zu verschlüsselnde Laufwerke zur Nutzung vorbereiten, müssen aber keine Berechtigung zum Einsehen der Daten haben. Das schützt sie im Verdachtsfall vor der Beschuldigung, sie hätten Dateninhalte preisgegeben.

Alle **3** Lösungen einzeln und in attraktiven Paketen erhältlich

digitronic® .net

vertrieb@digitronic.net ■ +49 371 81539-0