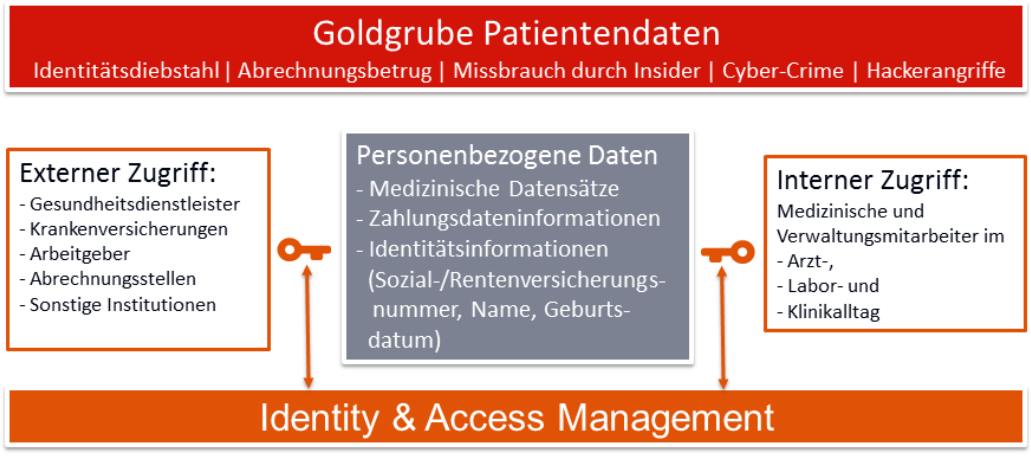
betasystems

Ein durchgängiges Identity-Management reduziert nicht nur die Kosten im IT-Support, sondern schützt auch sensible Informationen und IT Applikationen vor unberechtigten Zugriff. Viele Mitarbeiter und externe Partner haben über diese Systeme Zugriff auf äußerst sensible und personenbezogene Daten, die nicht in die Hände von Unbefugten gelangen dürfen!

Schützen Sie sensible Daten: Kontrollierter Zugriff auf Daten und Systeme für die Bereiche Medizin, Pflege und Verwaltung

Patientendaten sind sogar begehrter als Kreditkartendaten, da diese einzigartig sind und nicht einfach gesperrt werden können. Gesundheitsdaten sind daher ein exponiertes Ziel für Diebstahl und Missbrauch und je mehr IT in den Arzt-, Labor- und Klinik-Alltag Einzug hält, desto mehr sensible Daten entstehen.

Der Diebstahl von Gesundheitsdaten bietet ein breites Spektrum krimineller Möglichkeiten. Von Abrechnungsbetrug bis Identitätsdiebstahl können schwerwiegende Schäden entstehen. Umso wichtiger wird es, den Zugriff auf diese Daten durch eine Berechtigungsverwaltung zu schützen.



Eine benutzerfreundliche Berechtigungsverwaltung regelt zentral in den Gesundheitsorganisationen, welche Mitarbeiter/externen Geschäftspartner mit welchen Systemen arbeiten und welche sensiblen Informationen sie dabei einsehen dürfen. Auf Basis ihres Aufgabenprofils werden den Nutzern die benötigten Zugriffsrechte zur Verfügung gestellt.

42,5% aller Datenverstöße finden im Gesundheitsbereich statt.* im Verlauf der letzten beiden Jahre meldeten 91% aller Gesundheitsunternehmen, von mindestens einem Datenverstoß betroffen gewesen zu sein.

**Identity Theft Resource Center*

Warum sollten Sie sich für Beta Systems' IAM for HEALTHCARE entscheiden?

Erhöhte Datensicherheit durch optimierten Zugriffsschutz nach dem „Need-to-Know-Prinzip"

- **Einhaltung von Compliance Vorschriften hinsichtlich der schützenswerten Gesundheitsdaten** gemäß der Richtlinie zur Netzwerk- und Informationssicherheit (NIS) der Datenschutzgrundverordnung (GDPR) der EU und des §203 StGB zur ärztlichen Schweigepflicht, dem Schutz medizinischer Daten vor unberechtigter Einsichtnahme, auch durch Administratorenzugriffe.
- **Sicherheit durch die durchgängige Kontrolle der Vergabe von Anwenderrechten** - von der Beantragung bis zur technischen Einrichtung im IT-System.
- **Rollenbasierte Zugriffsberechtigungen** sichern den erforderlichen Informationszugang im Krankenhausbetrieb und steigern die Effizienz. Jeder erhält nur Berechtigungen für die Daten und Applikationen, die für die tägliche Arbeit benötigt werden.
- Patienten wechseln häufig die Abteilungen. Die daraus resultierenden notwendigen Aktualisierungen der Berechtigungen lassen sich automatisch in jede Anwendung übernehmen und **erhöhen so die Patientendatensicherheit.**
- **Digitale Antrags- und Verwaltungsprozesse** können aus den Fachbereichen heraus bedient und konfiguriert werden. Schnelle und sichere Einrichtung individueller Zugangsrechte auf aktuelle Datensätze der Patienten und die Ergebnisdaten der Diagnostik über berechtigungskontrollierte Workflows.
- **Funktionen zur Selbsthilfe entlasten die IT-Abteilung**: Einbindung eines zentralen Passwort Management Systems mit mobiler und E-Mail PIN erhöhen die Passwortsicherheit und reduzieren die Helpdesk-Kosten.
- Abdeckung zukünftiger Anforderungen durch Verbindung des IAM Systems mit Medizingeräten oder **neue Internet der Dinge** (IoT) Anwendungen im Gesundheitswesen.
- Verbesserte **Unterstützung am Point of Care**: Steuerung der Zugriffsberechtigungen auf die elektronische Patientenakte während der ‚digitalen Visite'.
- Business Intelligence basierte Berichte und Analysen ermöglichen die **schnelle Identifizierung der Bereiche, in denen ein hohes Zugriffsrisiko** besteht.
- **Alle** IT-Systeme lassen sich an unsere **zentrale Nutzerverwaltung** anbinden. Die Spanne reicht dabei von typischen Healthcare Applikationen wie etwa dem **Krankenhausinformationssystem (KIS)** sowie **Labor- (LIS)** und **Radiologie (RIS)-Informationssystem** bis hin zu Standard-IT Systemen wie dem Microsoft Verzeichnisdienst Active Directory.
- Das Identity Management wird **mit dem Personalmanagementsystem verknüpft**. Die übernommenen Mitarbeiterdaten sind somit stets aktuell. Inkonsistenzen werden dadurch verhindert.

Cyber-Crime im Gesundheitssektor

- Laut KPMG waren in den vergangenen zwei Jahren **81% aller großen Krankenhäuser und Krankenkassen** von Datenlecks betroffen.
- Mehr als 50% der Angriffe im Gesundheitssektor kamen von Insidern.
- **112 Millionen Gesundheitsdatensätze** wurden in 2015 in den USA gestohlen.
- Für 36% aller Betroffenen führte dies zu **finanziellen Schäden.**
- **Ø Profit pro medizinischer Identity Information $20.000**, d.h. 10x so hoch wie bei entwendeten Kreditkartendaten.
- Es dauert **2x so lange, Betrug** mit medizinischen Daten **aufzudecken** wie Kreditkartenbetrug.

Nehmen Sie Kontakt auf!

Beta Systems IAM Software AG

Josef-Lammerting-Allee 14
50933 Köln, Germany

+49 (0) 221 650 15 155, iam@betasystems.com

www.betasystems-iam.de

© Beta Systems, 2016