caradigm™
a Microsoft | GE Healthcare company

Caradigm™ Identity and Access Management

CASE STUDY

Ärzte und Pflegekräfte der Zentralen Notaufnahme im Zollernalb Klinikum sparen mit Caradigm Single-Sign-On täglich bis zu zwölf Stunden beim An- und Abmelden am PC

Identity and Access Management-Lösung von Caradigm unterstützt einen sicheren und schnellen Zugriff auf die Patientendaten über verschiedene Arbeitsplätze hinweg

Die Herausforderungen

Das Zollernalb Klinikum und Waldemar Potratz (Leiter SAP- & IT-Basis) standen 2013 vor zwei Herausforderungen: zum einen galt es, den hohen Anforderungen an den Datenschutz gerecht zu werden, zum anderen sollte den Ärzten und Pflegekräften gleichzeitig ein schneller und einfacher Zugang zu den Patientendaten ermöglicht werden. „Im Zuge der Neuausschreibung unseres Krankenhaus-Informationssystems (KIS) hat unser Datenschutzbeauftragter anwenderbezogene Anmeldungen zu den IT-Systemen gefordert, was den Mitarbeiter auf den Stationen aber nicht viel Zeit kosten durfte“, erläutert Potratz.

Ziel war es, gemäß den Anforderungen der Orientierungshilfe Krankenhaus-Informationssystem (OH KIS) zu arbeiten. „Ohne individuelle Anmeldung können wir zwar unbefugte Zugriffe feststellen, sie aber nicht identifizieren“, so Potratz. Vor Einführung der neuen Lösung haben häufig mehrere Mitarbeiter mit einem Zugang gearbeitet, der geöffnet war, solang die Zugriffsrechte ausreichten. Häufig hörte man das Argument, dass das ständige An- und Abmelden an verschiedenen Informationssystemen viel zu zeitaufwendig sei, und diese Zeit letztendlich bei der Versorgung der Patienten fehle.

„Deshalb sollte die Lösung einen schnellen Benutzerwechsel ermöglichen“, erläutert Potratz. „Mit Single-Sign-On (SSO) ist das An-, Um- und Abmelden schnell und sicher möglich. So können wir reibungslose Arbeitsabläufe im Stationsalltag gewährleisten.“

Die Lösung

Anfang November 2014 hat die ZNA in Balingen Caradigm Single-Sign-On als erste Abteilung im Zollernalb Klinikum eingeführt. „Dort haben die Ärzte und Pflegekräfte den größten Leidensdruck“, begründet Potratz die Entscheidung. „Sie müssen sich besonders häufig an- und abmelden, und das in teils schneller Folge.“ Hinzu kommt, dass in der ZNA bei jeder Behandlung fünf Informationssysteme geöffnet werden – neben dem KIS das Spezialsystem für die Notaufnahme, das Labor-Informationssystem, das Bilddaten-Managementsystem und das digitale Diktat.

Bei der ersten Anmeldung konfiguriert der Nutzer selbstständig seinen Chip, den er bereits für die Einlasskontrolle und Zeiterfassung einsetzt, mit Benutzernamen und Passwort. Die sind dann der Stempelchip-ID zugeordnet. „Das erspart

Zollernalb Klinikum gGmbH

Kunde: Zollernalb Klinikum
Anzahl der Betten: 510
Anzahl der Mitarbeiter: 1.200
Anzahl der Patienten stationär und ambulant: ca. 90.000
Land: Deutschland
Website: www.zollernalb-klinikum.de

“Caradigm SSO leistet einen wichtigen Beitrag zur Sicherheit. Die Lösung gewährleistet ein schnelles und sicheres An-, Um- und Abmelden und sorgt so für reibungslose Arbeitsabläufe im Stationsalltag.”

Waldemar Potratz
Leiter SAP- & IT-Basis,
Zollernalb Klinikum

“In der Notaufnahme geht es oftmals sehr hektisch zu, da zählt jede Sekunde. Mit Caradigm SSO sparen wir alleine für das An- und Abmelden an den Informationssystemen pro Schicht vier Stunden – Zeit, die Ärzte und Pflegekräfte in die Betreuung der Patienten investieren können.”

Dr. Katharina Schmid
Leitende Ärztin Zentrale Notaufnahme,
Zollernalb Klinikum

„Für die reibungslose Einführung hat auch Caradigm seinen Beitrag geleistet. Alle Zusagen wurden verlässlich eingehalten. Unser Ansprechpartner ist sehr häufig vor Ort und steht für alle Fragen und Erweiterungen zur Verfügung. Wir haben bis heute nicht das Gefühl, die Projektphase verlassen zu haben.“

Waldemar Potratz
Leiter SAP- & IT-Basis,
Zollernalb Klinikum

Caradigm™ Identity and Access Management

uns eine Menge administrativer Arbeit, zumal das Kennwort auch vom Nutzer selber über eine Sicherheitsfrage zurückgesetzt werden kann“, freut sich der IT-Leiter.

Bei Dienstbeginn legt der Anwender diesen Chip kurz auf ein Lesegerät, gibt sein Passwort ein und hat dann für zehn Stunden Zugriff auf alle Systeme, für die er berechtigt ist. Ab der zweiten Anmeldung entfällt die Eingabe des Passworts. Bei Verlassen des PCs muss nur noch die Chipkarte an das Lesegerät gehalten werden und die Sitzung wird getrennt, die Anwendungen werden aber im Hintergrund noch eine halbe Stunde aktiv gehalten. „Ich wechsle häufig den Arbeitsplatz. Da kommt es mir entgegen, dass nicht bei jeder Anmeldung wieder alle Systeme geladen werden müssen“, nennt Dr. Katharina Schmid, Leitende Ärztin in der Zentralen Notaufnahme, einen Vorteil dieses Vorgehens.

Vorteile & Nutzen

Bei der hohen Belastung von Ärzten und Pflegekräften zählt jede Sekunde, besonders in den Ambulanzen und in der Zentralen Notaufnahme (ZNA). Dort arbeiten immer zwölf Pflegekräfte und fünf Ärzte. Für eine saubere Windows-Anmeldung benötigen die Mitarbeiter zehn Sekunden, für das Einloggen in jedes weitere Informationssystem – das KIS, das Labor-Informationssystem und das Notaufnahme-Informationssystem - fünf Sekunden weniger durch SSO. Pro Anmeldevorgang kommen so 25 Sekunden zusammen. Bei 17 Mitarbeitern und durchschnittlich 35 An- und Abmeldungen erspart das Single-Sign-On den Beschäftigen also etwa vier Stunden pro Schicht. „Die gewonnene Zeit durch die SSO-Lösung investieren wir in die Entlastung der Mitarbeiter und die Behandlung unserer Patienten“, sagt Dr. Schmid.

„Ein Weiterer Vorteil besteht darin, dass das Sicherheitskonzept eine Zwei-Faktor-Authentifizierung vorsieht. Unsere Anwender müssen sich also nur noch ein Passwort merken, alles andere übernimmt die SSO-Lösung. Das beschleunigt den Benutzerwechsel speziell im klinischen Alltag mit einem hohen Patientendurchsatz deutlich“, so Potratz.

„Wenn ich mich persönlich anmelde, wird auch nur das lückenlos dokumentiert, was ich mache und anordne. Dieses Wissens ist für mich und meine Kollegen sehr wichtig. Fast noch bedeutender ist aber die Möglichkeit, sich schnell abzumelden und somit seinen Bildschirm vor unbefugten Zugriffen zu schützen“, erläutert Dr. Schmid.

Sowohl Potratz als auch Dr. Schmid stellen heraus, dass Caradigm Single-Sign-On klinikweit eine hohe Akzeptanz genießt. „Ob des erhöhten Zeitaufwands für die datenschutzkonformen An- und Abmeldungen haben wir mit einer gewissen Ablehnung des Verfahrens gerechnet. Dank SSO ist das heute kein Thema, eher im Gegenteil: „Die Mitarbeiter schätzen den Komfort der einfachen chipbasierten Anmeldung“, so der IT-Leiter.

Die Zukunft

Ist Caradigm Single-Sign-On flächendeckend eingeführt, würde Potratz sich gerne einem weiteren Thema nähern, der einfachen Benutzerverwaltung. Ein automatisches Erstellen und Verwalten von Benutzerkonten wie Zugriffsrechten würde der Personal- und der IT-Abteilung viel Arbeit und Zeit ersparen. „Wir könnten bestimmten Berufsgruppen definierte Rollen und Stationssichten zuweisen und diese dann automatisch bei neuen Mitarbeitern übertragen. Das verringert nicht nur den administrativen Aufwand, sondern optimiert auch das Informations- und Krankenhausmanagement. Nicht zuletzt – und das ist das Entscheidende – sparen die Ärzte und Pflegekräfte Zeit“, führt Waldemar Potratz aus.

Kundenprofil

Das Zollernalb Klinikum hat zwei Standorte, einen in Balingen und einen im knapp 20 Kilometer entfernten Albstadt. 2004 wurde zu Betrieb eine gemeinnützige Gesellschaft vom Zollernalbkreis und dem Universitätsklinikum Tübingen gegründet.
Seit April 2009 befinden sich die Häuser in alleiniger Trägerschaft des Landkreises.
Die Zollernalb Kliniken sind Häuser der Basisversorgung und halten Abteilungen der Inneren Medizin, Chirurgie, Gynäkologie und Geburtshilfe, Anästhesiologie und Intensivmedizin, Radiologie sowie Belegabteilungen für HNO, Augenheilkunde und Mund-Kiefer-Gesichtschirurgie vor.
Neben der breiten Basisversorgung verfügt das Klinikum über spezialisierte Schwerpunkte in der Kardiologie/Angiologie, Viszeral- und Gefäßchirurgie (Albstadt), in der Gastroenterologie, Diabetologie/Endokrinologie, Rheumatologie, Onkologie/Hämatologie und Unfallchirurgie und Orthopädie (Balingen).

KONTAKT

Caradigm Deutschland Ltd.

Adresse: Große Elbstraße 38
22767 Hamburg

Telefon: +49 (0)40 226 338 690

E-Mail: info@caradigm.de

Web: www.caradigm.de

caradigm™
a Microsoft | GE Healthcare company

Zugriffsmanagement für elektronische Patientendaten im Krankenhaus

Rechtliche Anforderungen und praktische Lösungen

Gliederung

Die tägliche Herausforderung

Ärzte und Pfleger leiden heutzutage gleichermaßen unter dem stetig ansteigenden Zeitdruck im klinischen Alltag, sei es im Notfallbereich, in den Ambulanzen oder auf den Stationen. Der Zeitdruck wird durch klinikintern vorgeschriebene, mitunter langwierige An- und Abmeldeprozesse an Klinikcomputern zusätzlich erhöht. Die Log-in und Log-out Vorgaben erscheinen dabei unumgänglich, will man den (datenschutz-)rechtlichen Vorgaben entsprechen. Durch vermeintlich pragmatische Lösungen kann es im Krankenhausalltag aber häufig zu Umgehungen der (datenschutz-)rechtlichen Vorgaben kommen.

Beispiel 1: Die Sammelbenutzerkennung

Der in der Notfallambulanz eingeteilte leitende Oberarzt hält es für viel zu zeitaufwendig, sich an unterschiedlichen Arbeitsplätzen mit seiner Benutzerkennung und seinem Passwort stets erneut einzuloggen. Er ist der Ansicht, der hohe Durchlauf an Patienten und die Vielzahl an Behandlungsräumen in der Rettungsstelle erlaubten es nicht, durch das zeitintensive Ein- und Ausloggen wertvolle Zeit zu verlieren. Zeit bedeute in der Rettungsstelle schließlich Leben. So teilt er allen in der Rettungsstelle tätigen Ärzten sowie dem Pflegepersonal mit, dass nur noch seine Kennung als eine gemeinsame Benutzerkennung verwendet werden solle. Ein An- und Abmelden sei nicht mehr notwendig. Da er mit seiner Kennung zugleich Zugriff auf Patientinnen der gynäkologischen Station hat, können nun auch alle anderen auf diese Daten zugreifen. Eine Krankenschwester durchsucht daraufhin elektronische Krankenakten der gynäkologischen Station und entdeckt, dass eine ihrer Kolleginnen schwanger ist.

Beispiel 2: Das vergessene Ausloggen

Der für die dermatologische Abteilung eingeteilte PJ-Student soll für einen Stationsarzt einen Arztbrief entwerfen. Er setzt sich an den PC im Arztzimmer und sieht, dass das System bereits online ist. Der Chefarzt der Onkologie hat vergessen sich abzumelden. Ein eigenes Einloggen hält der PJ-Student daher für entbehrlich. So verwendet er den Zugang des Chefarztes der Onkologie und stößt dabei auf den zuletzt geöffneten Patienten. Dabei stellt er fest, dass einer seiner Professoren sich zur stationären Behandlung in der onkologischen Abteilung befindet. Er ist an Bauchspeicheldrüsenkrebs erkrankt und hat nur noch wenige Monate zu leben.

Beispiel 3: Die neue Krankenschwester

Eine neue Krankenschwester beginnt in der Abteilung für Innere Medizin des Krankenhauses zu arbeiten. Da die Erfahrung zeigte, dass die IT-Abteilung meist mehrere

Tage benötigt, um für neue Mitarbeiter einen eigenen Account für das Krankenhausinformationssystem zu erstellen, nennt der Stationsarzt der neuen Schwester kurzerhand seine eigenen Kenndaten zur „vorläufigen“ Nutzung und verabschiedet sich in seinen Urlaub. Die neue Krankenschwester loggt sich in der Folge mehrere Tage lang mit der Arzt-Kennung ein. Wenig später verlangt eine Patientin Auskunft, an wen ihre Daten innerhalb der Klinik weitergeben werden. Dabei fallen dem betrieblichen Datenschutzbeauftragten die zahlreichen Zugriffe des Stationsarztes während seiner Abwesenheit auf. Darauf angesprochen, ob die Schwester zugegriffen habe, bestreitet diese die Zugriffe. Die Auskunft des Krankenhauses gegenüber der Patientin ist daher ungenügend.

Konflikte zwischen Compliance und Effizienz

Klinikinterne Datenschutzvorgaben bestehen häufig darin, dass der Anwender für jede Session seine Kennungsdaten erneut eingeben muss, was mit einem nicht unbeachtlichen Zeit- und Konzentrationsaufwand einhergeht. Wie die Beispielsfälle zeigen, können solche Vorgaben dazu führen, dass im Klinikalltag zwingendes Recht nicht eingehalten wird. Dann drohen empfindliche Sanktionen, wie etwa Bußgelder, strafrechtliche Sanktionen, aber an erster Stelle der Verlust von Vertrauen und Glaubwürdigkeit gegenüber Patienten, Krankenkassen und Behörden.

Den Konflikt zwischen möglichen Effizienzvorgaben der Geschäftsführung und datenschutzrechtlichen Compliancevorgaben spüren in der Regel besonders deutlich die Mitarbeiter der IT-Abteilungen in den Krankenhäusern.

Zum einen fordert die Krankenhausleitung regelmäßig dazu auf, die An- und Abmeldevorgänge zu beschleunigen, um den performanten Arbeitsfluss im klinischen Umfeld zu fördern. Zugleich soll das Anlegen neuer Benutzer ohne Vorlaufzeit ermöglicht werden, um neue Mitarbeiter unmittelbar einsetzen zu können.

Zum anderen wird die IT-Abteilung immer wieder durch die betrieblichen Datenschutzbeauftragten der Klinik ermahnt, die datenschutzrechtlichen Vorgaben einzuhalten. In jüngerer Zeit geschieht dies häufig unter Verweis auf die Kontrolltätigkeit der deutschen Datenschutzbehörden in Bezug auf Krankenhausinformationssysteme und die von den Datenschutzbehörden verfasste „Orientierungshilfe-Krankenhausinformationssysteme“ (OH-KIS). Im Wesentlichen gelten dabei folgende rechtliche Grundsätze:

Personenbezogene Gesundheitsdaten unterliegen den Regelungen des Datenschutzrechts. Abhängig von der Trägerschaft eines Krankenhauses können für deutsche Krankenhäuser unterschiedliche Datenschutzgesetze gelten. Während Krankenhäuser in privater Trägerschaft dem Bundesdatenschutzgesetz – BDSG – unterliegen, gelten für Krankenhäuser in öffentlicher Trägerschaft der Länder die jeweiligen Datenschutzgesetze der Länder und/oder speziellere datenschutzrechtliche Regelungen der Landeskrankenhausgesetze. Krankenhäuser in christlich-kirchlicher Trägerschaft unterliegen den Datenschutzgesetzen der jeweiligen (protestantischen oder katholischen) Kirche.

Die deutschen **Datenschutzbehörden** haben am 16./17. März 2011 im Rahmen der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Würzburg die sog. **Orientierungshilfe Krankenhausinformationssysteme („OH KIS“)** beschlossen. Diese enthält sowohl rechtliche als auch technische Vorgaben. Hiernach müssen beispielsweise die Zugriffsrechte des Einzelnen auf seine konkrete Aufgabe im Krankenhaus begrenzt werden. Die deutschen Datenschutzbehörden haben besonders hervorgehoben, dass Patientendaten nicht vom gesamten Krankenhauspersonal eingesehen werden dürfen, sondern nur in Abhängigkeit zu einem tatsächlichen Erfordernis der Kenntnisnahme, das von der jeweiligen Rolle der Person abhängt (**„rollenbasierte Zugriffsrechte“**, vgl. OH KIS Nr. 10 Normative Eckpunkte).

Zu den **Prinzipien des Datenschutzrechts** gehört es auch, dass Krankenhäuser als Einrichtungen, die personenbezogene Daten verwenden, angemessene technische und organisatorische Maßnahmen treffen müssen. Die **Anlage zu § 9 Satz 1 BDSG** nennt Kriterien für solche Maßnahmen. So sind Maßnahmen zu treffen, die beispielsweise dazu geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten benutzt werden können **(Zugangskontrolle, Nr. 2)**. Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle, Nr. 3)**. Eine notwendige **Eingabekontrolle** fordert, dass

nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Auf die Notwendigkeit der Protokollierung weist auch die OH KIS ausdrücklich hin (vgl. OH KIS Nr. 37 Normative Eckpunkte und Nr. 7 Technische Anforderungen).

Die Nachvollziehbarkeit und Vollständigkeit der elektronischen Patientenakte dient zudem dem zwischenzeitlich in § 630g BGB ausdrücklich geregelten **Recht des Patienten auf Einsichtnahme** in die Patientenakte.

Das Bundesamt für Sicherheit in der Informationstechnik hält es auch für eine nützliche Maßnahme, den Bildschirm nach einer bestimmten Zeit der Inaktivität zu sperren (Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzkataloge, Maßnahmenkataloge, M 4.2 **Bildschirmsperre**). Es stellt auch Regeln zum **Passwortgebrauch** auf (Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzkataloge, Maßnahmenkataloge, M 2.11 Regelung des Passwortgebrauchs). Danach müssen Passwörter geheim gehalten werden und sollten nur dem Benutzer persönlich bekannt sein.

Mediziner müssen über das, was ihnen in ihrer Eigenschaft als Arzt oder Ärztin anvertraut oder bekannt geworden ist, schweigen (vgl. § 9 Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä). Sie dürfen die Patientengeheimnisse nur dann offenbaren, wenn dies durch eine gesetzliche Vorschrift oder aufgrund einer Einwilligung des Patienten oder aber aufgrund überwiegender Interessen gerechtfertigt ist. Das **ärztliche Berufsgeheimnis** ist nicht nur im ärztlichen **Berufsrecht** normiert, sondern wird auch durch das deutsche **Strafrecht** flankiert (§ 203 Strafgesetzbuch). Auch wenn diese Pflicht zur Geheimhaltung unmittelbar nur an die Ärzte und ihre Gehilfen adressiert ist, beeinflusst es zumindest auch indirekt die Arbeit von Krankenhäusern, da die Krankenhäuser als Arbeitgeber für ihre Arbeitnehmer verantwortlich sind.

Technische Lösungsmöglichkeiten

Der Konflikt zwischen IT-Compliance und Effektivität kann jedoch schon heute nach dem „state of the art“ durch technische Lösungen erheblich vermindert werden, die die Erfüllung der rechtlichen Vorgaben unterstützen, während sie gleichzeitig helfen, Zeit und Aufwand zu sparen, um klinische Workflows zu fördern.

Solche einheitlichen Systeme optimieren die Vorgänge des An- und Abmeldens, bieten darüber hinausgehende detaillierte, rollenbasierte Zugriffsberechtigungen für eine effiziente Arbeitsweise und unterstützen gleichzeitig die Einhaltung der rechtlichen Vorgaben.

Hierzu gehören Produkte, die die folgenden Lösungen beinhalten:

1. Single Sign On und automatisches Ausloggen

Eine zeitsparende Maßnahme ist das einmalige Anmelden des klinischen Mitarbeiters an seinem Arbeitsplatz mit seinem Benutzernamen und seinem Kennwort. Wechselt er nun seinen Arbeitsplatz, genügt es bei solchen IT-Lösungen, wenn der Mitarbeiter sich am neuen Arbeitsplatz authentisiert. Der Mitarbeiter wird dadurch automatisch am neuen Arbeitsplatz in das bereits angemeldete System eingeloggt (sog. Single Sign On). Die Verwendung von Erkennungsgeräten wie Chipkarte, Token, Fingerabdruck oder Irisscanner erhöht die Anwenderfreundlichkeit und ermöglicht den Zugang zu Desktops und Applikationen ohne die erneute Eingabe von Kenndaten.

Im Zusammenhang mit dem Prinzip des Single Sign On ist auch eine umfängliche Abmelde-Systematik sinnvoll, wonach ein einmaliges Abmelden genügt, um alle geöffneten Anwendungen inkl. aller weiteren geöffneten Fenster zu schließen. Sollte ein solcher Log-out nicht durchgeführt werden und verlässt der Anwender den Arbeitsplatz, empfiehlt sich der Schutzmechanismus der Zeitschaltung. Hierdurch kann vermieden werden, dass die Session des Anwenders von Anderen benutzt wird. Praxisnahe Lösungen, die individuell bestimmbare, beispielsweise User-Gruppen-bezogen Auslog-Zeiten zulassen, sind hierbei hilfreich. Dadurch können sinnvollerweise in Abteilungen mit hohem Traffic (z.B. Notfallambulanz) kurze automatische Auslog-Zeiten bestimmt werden, wohingegen in publikumsarmen Bereichen (z.B. Einzelbüros) die Zeiten länger sein können.

2. Context-Management

Häufiges Ein- und Ausloggen kann auch einen Verlust an Konzentration zur Folge haben. Hinzu kommt, dass die Behandlung vieler verschiedener Patienten in kurzer Zeit zu Ungenauigkeiten in den Arbeitsabläufen führen kann. Die Gefahr versehentlich Patientendaten zu verwechseln, kann durch ein Context-Management-System minimiert werden, das die Anzeige eines Patienten in allen Applikationen erlaubt. Solche Systeme ermöglichen gegenüber Einzelaufrufen in verschiedenen Applikationen Zeitersparnisse und mehr Sicherheit gegen Verwechslungsgefahr.

3. Passwort-Reset

Die technische Möglichkeit des Anwenders, sein Passwort selbst, d.h. ohne Hinzuschalten eines Dritten (z.B. Helpdesk), zurücksetzen zu können, spart nicht nur Zeit und Ressourcen, sondern kann zudem sicherstellen, dass nur der Anwender – im Unterschied zum Einschalten eines Helpdesks – über seine Zugangsdaten verfügt.

4. Rollenbasiertes Erstellen neuer System-Accounts

Die Option, neue System-Accounts anhand bereits vorgefertigter Profile elektronisch generieren zu können, erlaubt das zentralisierte Erstellen, Modifizieren und Löschen rollenbasierter Zugriffsberechtigungen sowohl für Active Directory-Systeme (AD-Systeme) als auch für alle klinischen Systeme. Die Berechtigungen können abhängig von den Aufgaben des neuen Anwenders erteilt, modifiziert und gelöscht werden.

Dies führt neben einer schnellen, taggenauen Handlungsfähigkeit des neuen Anwenders auch zur Verhinderung eines verfrühten Herausgebens der Account-Daten an den neuen Anwender und macht ein datenschutzrechtlich bedenkliches „vorläufiges“ Nutzen von fremden Systemzugängen überflüssig. Außerdem kann hierdurch eine klinikweit einheitliche Account-Struktur für bestimmte Berufsgruppen und Abteilungen erreicht werden, wodurch einem versehentlichen Herausgeben von zu weitreichenden Zugängen entgegen gewirkt wird. Das umfassende Deaktivieren aller System-Accounts eines Anwenders verhindert nach einem Ausscheiden eines Mitarbeiters die Gefahr, dass unbeabsichtigt Alt-Accounts aktiv bleiben und von Unbefugten verwendet werden können.

5. Protokollierung & Audit Funktionen

Durch integrierte Protokollierungs-Funktionen kann überprüft werden, welche Nutzer wann welche Anwendungen und Patienten aufgerufen haben. Die Protokollierung dient dazu, unberechtigte Datennutzung – auch nachträglich – aufspüren zu können und dem Patienten auf Wunsch umfangreiche Informationen über die Verwendung seiner Daten zukommen zu lassen.

Zeitgemäße Zugriffs- und Managementsysteme erleichtern das Ein- und Ausloggen steigern den Workflow und mindern das Verlangen nach Sammelbenutzerkennungen im klinischen Alltag **(Beispiel 1)**. Die modernen Verfahren zum automatischen Ausloggen helfen zudem unberechtigte Zugriffe zu verhindern **(Beispiel 2)**. Anwenderfreundliche Verfahren zur Erstellung neuer System-Accounts mindern das Risiko der Nutzung fremder Accounts und erleichtern die adäquate Auskunft gegenüber Patienten, wer auf ihre Daten zugegriffen hat **(Beispiel 3)**.

Für die in diesem Dokument beschriebenen datenschutzrechtlichen Herausforderungen bietet Caradigm mit der Identity und Access Management Suite unterschiedliche Lösungsansätze für den Zugriff auf Patientendaten.

Disclaimer:

Dieses Dokument wurde mit der Unterstützung von Dierks + Bohle Rechtsanwälte erstellt.

DIERKS + BOHLE
RECHTSANWÄLTE

Dieses Dokument ist Eigentum von Caradigm und darf nicht weiterverbreitet werden. Es dient ausschließlich Informationszwecken und alle Abbildungen oder Beispiele sind rein fiktiv. Dieses Dokument enthält keine Zusage, Garantie oder Verpflichtung hinsichtlich der enthaltenen Produkte oder Dienstleistungen und beinhaltet keinen Rechtsrat. Caradigm steht nicht dafür ein, dass die Produkte und Dienstleistungen von Caradigm alle datenschutzrechtlichen Anforderungen unter allen Umständen erfüllen. Die Merkmale und Konfigurationen Ihres Produkts können vom Dargestellten abweichen und abhängig vom Markt- und Vertriebsort variieren. Beschreibungen zukünftiger Funktionen geben den aktuellen Produktionsstand wieder und stellen keine Verpflichtung hinsichtlich der Verfügbarkeit einer bestimmten Funktion dar. Zeitplan und Verfügbarkeit stehen im Ermessen von Caradigm und unterliegen Änderungen sowie den notwendigen behördlichen Genehmigungen. Namen von Personen, Einrichtungen und Orten sowie damit verbundene Informationen sind fiktiv. Jede Ähnlichkeit zu tatsächlichen Personen, Einrichtungen oder Orten ist rein zufällig.

Rechtliche Vorschriften

§ 3 Abs. I, 9 Bundesdatenschutzgesetz – BDSG:

„(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

[...]

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) [...]“

§ 4 Abs. I Bundesdatenschutzgesetz – BDSG:

“(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) [...]“

§ 9 Bundesdatenschutzgesetz – BDSG:

„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Anlage zu § 9 Satz I Bundesdatenschutzgesetz – BDSG:

„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.“

§ 203 Strafgesetzbuch – StGB

„(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,

   [...]

   anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

[...]

(3) [...] Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlaß erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.“

§ 9 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (Stand 2011)

„(1) Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist - auch über den Tod der Patientin oder des Patienten hinaus - zu schweigen. Dazu gehören auch schriftliche Mitteilungen der Patientin oder des Patienten, Aufzeichnungen über Patientinnen und Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

(2) Ärztinnen und Ärzte sind zur Offenbarung befugt, soweit sie von der Schweigepflicht entbunden worden sind oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. Soweit gesetzliche Vorschriften die Schweigepflicht der Ärztin oder des Arztes einschränken, soll die Ärztin oder der Arzt die Patientin oder den Patienten darüber unterrichten.

(3) Ärztinnen und Ärzte haben ihre Mitarbeiterinnen und Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

(4) Wenn mehrere Ärztinnen und Ärzte gleichzeitig oder nacheinander dieselbe Patientin oder denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis der Patientin oder des Patienten vorliegt oder anzunehmen ist.“

DIERKS + BOHLE Rechtsanwälte
Kurfürstendamm 195
D - 10707 Berlin

Tel. +49 30 327787-0
Fax +49 30 327787-77

http://www.db-law.de
office@db-law.de

Caradigm Deutschland Ltd.
Große Elbstraße 38
D - 22767 Hamburg

Tel.: +49 40 18 19 28 61

info@caradigm.de
www.caradigm.de

caradigm™
a Microsoft | GE Healthcare company

Caradigm™ Identity and Access Management

IT-Abteilungen von Krankenhäusern stehen mittlerweile vor großen Herausforderungen: Auf der einen Seite müssen sie einen konstanten, effizienten Datenzugriff bei einer steigenden Anzahl klinischer, administrativer und mobiler Anwendungen gewährleisten, auf der anderen Seite kämpfen sie mit einer stetig wachsenden Datenmenge sowie einem erhöhten Planungsbedarf aufgrund einer vermehrt flexibel einsetzbaren Belegschaft über Krankenhausgrenzen hinweg.

Prozesse vereinfachen

Caradigm ermöglicht Krankenhäusern einen direkten und schnellen Zugriff auf Patientendaten ohne langwierige Anmeldeprozesse und ohne unzählige Klicks, bis man den richtigen Patienten gefunden hat. Caradigm konzentriert sich ausschließlich auf das Gesundheitswesen und bietet somit optimal zugeschnittene Lösungen sowohl für das klinische Personal als auch für die krankenhausinterne IT-Abteilung an.

Die IAM-Lösung ist nicht nur für die Passwortverwaltung zuständig, sondern unterstützt auch gleichzeitig Krankenhäuser bei weiteren Herausforderungen, z. B. Zugriffsberechtigungen, Verfahrensverzeichnisse, Zugriffsdokumentation, Minderung klinischer Risiken am Computer, Optimierung klinischer Abläufe usw.. Somit kann der IT-Verwaltungsaufwand minimiert und die Einhaltung branchenspezifischer Vorschriften vereinfacht werden, sodass das klinische Personal sich auf die Patientenversorung konzentrieren kann.

Ein weiterer Vorteil ist, dass die Caradigm IAM-Suite modular oder als komplettes Lösungspaket implementiert werden kann und sich somit Betriebsaufwand und -kosten entsprechend reduzieren lassen können.

Caradigm IAM besteht aus folgenden Lösungen:

Caradigm Single-Sign-On (SSO) ermöglicht es Klinikmitarbeitern, sich mit denselben Zugangsdaten und mithilfe einer Multifaktor-Authentifizierung an verschiedenen klinischen Arbeitsplätzen schnell und einfach im System und danach automatisch in allen benötigten Applikationen anzumelden. Somit haben die Anwender schnellen Zugriff auf die benötigten Daten und müssen sich an den verschiedenen Arbeitsplätzen nicht jedes Mal wieder neu anmelden.

Die Caradigm Identity and Access Management Lösung unterstützt Gesundheitseinrichtungen dabei, den Benutzerzugriff auf Applikationen und Patientendaten effizient zu verwalten.

Vorteile

- Single-Sign-On und schneller Benutzerwechsel
- Kontextmanagement: immer den richtigen Patienten im Zugriff
- Rollenbasierter Zugriff und starke Authentifizierung
- Selbstständiger Passwort-Reset
- Automatisches Benutzermanagement/ Provisioning
- Einfache Einbindung von neuen Applikationen
- Umfangreiche Unterstützung für VDI-Umgebungen
- Zahlreiche Auditfunktionen

Caradigm™ Identity and Access Management

Caradigm Context Management sorgt dafür, dass in den verschiedenen Anwendungen immer derselbe Patientenkontext erhalten bleibt. Klinikmitarbeiter, die von einer Anwendung zur nächsten wechseln müssen, können so automatisch auf die richtigen Patientendaten zugreifen, denn der aufgerufene Patient wird automatisch in den anderen Anwendungen im Hintergrund geöffnet und synchronisiert. Dies kann viel Zeit sparen und der Verwechslung von Patientendaten vorbeugen.

Caradigm Provisioning ist eine rollenbasierte Identitätsverwaltungslösung, mit der automatisch Benutzerkonten und Zugriffsrechte zu klinischen Anwendungen erstellt, modifiziert oder gesperrt werden können. Indem Pflegekräfte einen schnellen Zugriff auf die von ihnen benötigten Anwendungen und Daten erhalten, kann der administrative Aufwand verringert und das Informations- und Krankenhausmanagement optimiert werden.

Funktionen

- Diverse starke Authentifizierungsmöglichkeiten
- Rollenbasierte Taskleiste
- Organisationsweites Single-Sign-On
- Klinikweites “Patienten Context Management”
- Rollenbasierte Zugriffsrechte
- Passwortsynchronisation
- „Privacy Auditor“, um die Einhaltung von Datenschutzrichtlinien zu unterstützen

UNTERNEHMENSPROFIL

Caradigm ist ein von Microsoft und GE Healthcare im Juni 2012 gegründetes Joint Venture und bietet Lösungen aus den Bereichen Population Health Management und Healthcare Analytics.

Die Lösungen des Unternehmens unterstützen Organisationen und Kostenträger im Gesundheitswesen dabei, Qualität und Wirtschaftlichkeit von Behandlungen kontinuierlich zu verbessern. Die offene Plattformlösung basiert auf Microsoft-Technologien und gibt Anwendern wertvolle Aggregations- und Analysewerkzeuge an die Hand. Des Weiteren ermöglichen die Caradigm Lösungen einen einfachen und schnellen Zugang zu den richtigen Daten und unterstützen somit einen effizienten Arbeitsablauf am klinischen Arbeitsplatz. Caradigm hilft Krankenhäusern, den steigenden Anforderungen von Patienten und Organisationen im Gesundheitswesen gerecht zu werden, Kosten zu reduzieren und Risiken zu vermeiden.

KONTAKT

Caradigm Deutschland Ltd.

Adresse: Große Elbstraße 38
22767 Hamburg

Telefon: +49 (0)40 302 378 80
Fax: +49 (0)40 302 379 82

E-Mail: info@caradigm.de

Web: www.caradigm.de

caradigm™
a Microsoft | GE Healthcare company