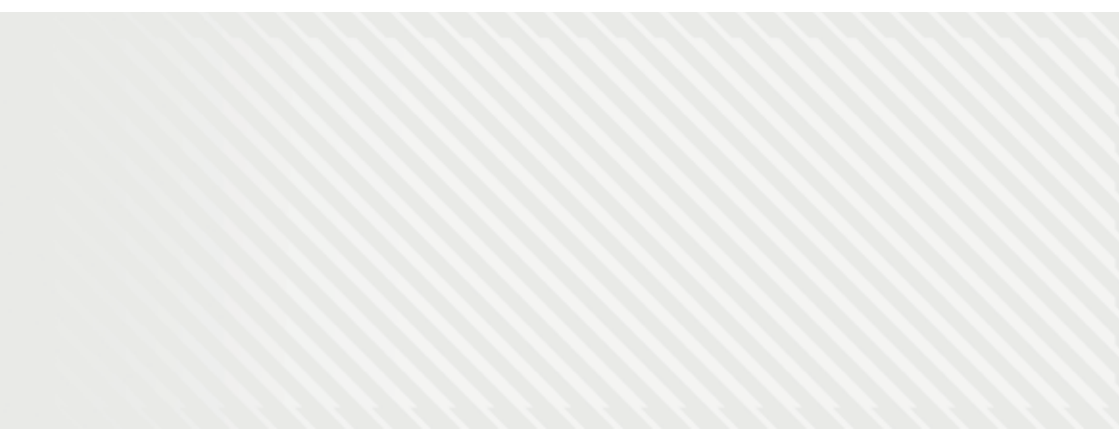




Zugriffsmanagement für elektronische Patientendaten im Krankenhaus

Rechtliche Anforderungen und praktische Lösungen



Ärzte und Pfleger sind heutzutage gleichermaßen einem stetig ansteigenden Zeitdruck im klinischen Alltag ausgesetzt, sei es in der Notaufnahme, in der Ambulanz oder auf Station. Der Zeitdruck wird durch mitunter langwierige An- und Abmeldeprozesse an Klinikcomputern zusätzlich erhöht. Die Log-in und Log-out-Vorgaben erscheinen dabei unumgänglich, will man den datenschutzrechtlichen Vorgaben entsprechen. Vermeintlich pragmatische Lösungen im Krankenhausalltag beinhalten jedoch häufig Umgehungen der datenschutzrechtlichen Vorgaben.

Den Konflikt zwischen möglichen Anforderungen der Geschäftsführung an die Effizienz und datenschutzrechtlichen Compliancevorgaben spüren in der Regel besonders deutlich die Mitarbeiter der IT-Abteilungen in den Krankenhäusern. Technische Lösungen nach dem „state of the art“ unterstützen die Erfüllung der rechtlichen Vorgaben, während sie gleichzeitig helfen, Zeit und Aufwand zu sparen, um klinische Workflows zu fördern. Sie können den Konflikt zwischen IT-Compliance und Effektivität **schon heute** erheblich mindern.

Einheitliche 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**.

Solche technischen Lösungsmöglichkeiten sind beispielsweise:

■ 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. 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.

Daneben sind anwenderspezifische Abmelde-Systeme sinnvoll, wonach ein einmaliges Abmelden genügt, um alle geöffneten Anwendungen zu schließen. Verlässt der Anwender den Arbeitsplatz ohne einen solchen Log-out, empfiehlt sich der Schutzmechanismus der User-Gruppen-bezogenen Zeitschaltung. Durch sie können in Abteilungen mit hohem Traffic (z.B. in der Notfallambulanz) besonders kurze automatische Auslog-Zeiten eingerichtet werden.

■ Context-Management

Die Gefahr, versehentlich Patientendaten zu verwechseln, kann durch ein Context-Management-System reduziert werden, das die Anzeige eines Patienten in allen Applikationen erlaubt. Solche Systeme ermöglichen gegenüber Einzelaufrufen in verschiedenen Applikationen Zeitersparnisse und mehr Sicherheit vor Verwechslungen.

■ 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.

■ 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. Das datenschutzrechtlich bedenkliche, aber im Klinikalltag regelmäßig auftretende „vorläufige“ Nutzen von fremden Systemzugängen wird dadurch überflüssig.

■ Protokollierung & Audit Funktionen

Durch integrierte Protokollierungs-Funktionen kann überprüft werden, welche Nutzer zu welcher Zeit 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.

Diese zeitgemäßen Zugriffs- und Managementsysteme erleichtern das Ein- und Ausloggen, steigern den Workflow und mindern das Verlangen nach Sammelbenutzerkennungen im klinischen Alltag. Die innovativen Verfahren zum automatischen Ausloggen helfen zudem, unberechtigte Zugriffe zu verhindern. Anwenderfreundliche

Verfahren zur Erstellung neuer System-Accounts mindern zudem das Risiko der Nutzung fremder Accounts und erleichtern die adäquate Auskunft gegenüber Patienten, wer auf ihre Daten zugegriffen hat.

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

Rechtliche Grundsätze

Personenbezogene Gesundheitsdaten unterliegen den Regelungen des Datenschutzrechts, wozu v.a. die Vorgaben des Bundesdatenschutzgesetzes (BDSG) gehören.

Die **Orientierungshilfe Krankenhausinformationssysteme („OH KIS“)** der Datenschutzbehörden enthält zudem 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**“).

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). 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**).

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.

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 **Bildschirm Sperre**). 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.

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.

Caradigm® ist eine eingetragene Marke von Caradigm. ©2013 Caradigm.
Alle Rechte bleiben vorbehalten.

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
