CGM LIFE

Sicherheit und Datenschutz

Daniel Bobbert
CompuGroup Medical Software GmbH

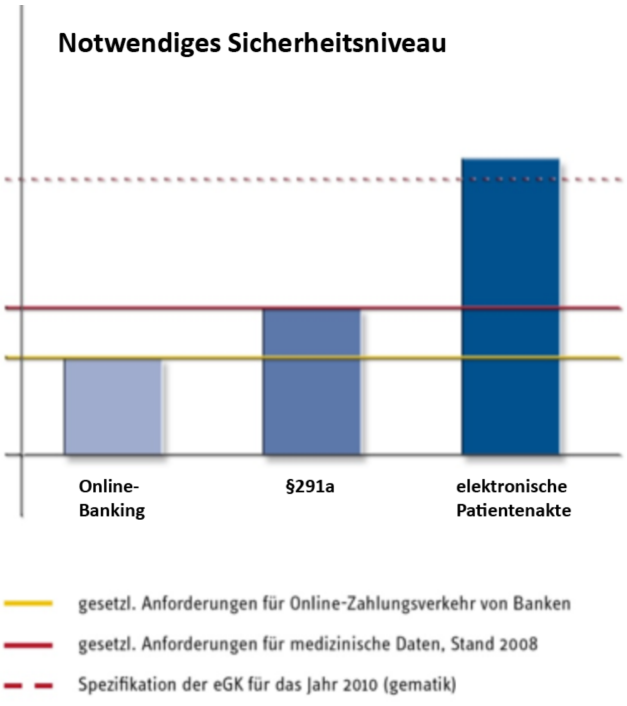
CGM LIFE – Sicherheit und Datenschutz

Das Wohl des Patienten steht immer an erster Stelle

Die elektronische Patientenakte CGM LIFE ermöglicht einen umfassenden und zielgerichteten Austausch medizinischer Daten zwischen Patienten, Ärzten und weiteren Leistungserbringern. In Zukunft geht der Trend unweigerlich in Richtung patientenbestimmter medizinischer Akten. Denn sie sind die Basis für sichere softwaregestützte medizinische Expertensysteme und helfen dabei Leben zu retten, Krankheiten zu heilen und Gesundheit zu erhalten. Selbstverständlich stehen Sicherheit und das Wohl der Patienten hierbei immer an erster Stelle. Um höchste Datensicherheit zu gewährleisten, werden Datenschutzverfahren auf Basis der neuesten internationalen Erfahrungen und Standards benötigt.

Grundlegende Sicherheitsphilosophie

Die geltenden Datenschutzgesetze stellen für den üblichen Geschäftsverkehr sicher, dass das Recht auf Selbstbestimmung und vor allem die Privatsphäre jedes Einzelnen jederzeit gewahrt bleiben.



Dabei gehen die Sicherheitsanforderungen für eine elektronische Patientenakte weit über die Anforderungen an Online-Banking oder andere, häufig als Vergleichsmaßstab herangezogene Dienste hinaus.

Die Gemeinsamkeiten bestehen zunächst darin, dass die Übertragung sämtlicher Daten zwischen Client und Server durch eine Transportverschlüsselung geschützt sein muss, und dass der Betreiber der Server die Sicherheit, Unversehrtheit und Verfügbarkeit der gespeicherten Daten garantieren muss, indem er den Zugriff auf die Daten durch Unbefugte unterbindet.

Der Betreiber der Akte darf selbst keinen Zugriff auf die Inhalte der Akte haben

Der entscheidende Unterschied besteht aber darin, dass der Anwender etwa beim Online-Banking Zugriff auf Daten nimmt, die auch im Zugriff des Betreibers selbst (in diesem Falle die Bank) sind. D.h. die Bank kennt den Kontostand, die ein- und ausgehenden Transaktionen, sowie persönliche Daten wie den Verwendungszweck einer Überweisung. Die elektronische Patientenakte hingegen speichert höchst sensible, personenbezogene Daten, die auch vor einem Zugriff durch den Betreiber der Server selbst geschützt werden müssen.

Die elektronische Patientenakte ist ein Schließfach, zu dem nur der Patient den Schlüssel besitzt

In diesem Sinne ist die elektronische Patientenakte besser mit einem Schließfach zu vergleichen, das zwar in der Obhut des Betreibers steht und durch diesen vor Manipulation geschützt wird, auf das der Betreiber selbst aber keinen Zugriff hat, weil nur der Besitzer den notwendigen Schlüssel besitzt.

Der Patient als alleiniger Besitzer der Akte hat die volle Verfügungsgewalt über seine persönlichen Daten. Er alleine entscheidet, wer zu welchem Zeitpunkt Zugriff auf die Daten in seiner Akte nehmen kann.

Verhinderung von gläsernem Arzt und gläsernem Patienten

Diese Sicherheit kann und muss durch technische Maßnahmen sichergestellt werden. Sie darf nicht von administrativen Regeln und dem Vertrauen in deren Einhaltung abhängen. Nur so kann der gläserne Patient und der gläserne Arzt wirksam und unwiderruflich verhindert werden.

Datenschutz- und Datensicherheits-konzept

Die Sicherheitsarchitektur der elektronischen Patientenakte CGM LIFE basiert genau auf diesen Grundlagen und implementiert damit einen wirksamen, unumgänglichen **technischen Beschlagnahmeschutz**, d.h. medizinischen alle Daten sind in CGM LIFE so verschlüsselt gespeichert, dass selbst mit Vollzugriff auf die CGM LIFE Server und Zugriff auf den Source Code eine Entschlüsselung der Daten durch Unbefugte technisch unmöglich ist.

Dieses Datenschutz- und Datensicherheitskonzept soll in den folgenden Abschnitten transparent dargestellt werden.

1.1 Grundlagen des Datenschutzes und der Datensicherheit

Geltungsbereich der Datenschutzgesetze

Die bestehenden Datenschutzgesetze gelten für alle elektronischen Anwendungen, so auch für die Verarbeitung von medizinischen Daten in einer elektronischen Patientenakte. Zusätzlich gelten die Regeln aus dem Ärzterecht hinsichtlich der ärztlichen Schweigepflicht.

Gesetzliche Regelungen zur Speicherung medizinischer Daten

Dieses Dokument berücksichtigt die geltenden gesetzlichen Regelungen, Hinweise, sowie Veröffentlichungen der nachfolgenden Institutionen zu technischen und rechtlichen Anforderungen an elektronische Patientenakten:

- Bundesbeauftragter für Datenschutz und Informationsfreiheit
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Landesbeauftragter für Datenschutz RLP
- LDI (Landesamt für Datenschutz und Informationsfreiheit NRW)
- Bundesärztekammer

Sicherheitsstruktur der elektronische Patientenakte CGM LIFE

Inhalt der elektronischen Patientenakte

Daten liegen in CGM LIFE in Form von Medizinischen Datenobjekten (MDO) vor. Diese umfassen strukturierte medizinische Daten zu Diagnosen, Medikamenten, Laborwerten, Befunden usw. Sowie unstrukturierte Daten, z.B. Bilddaten, Arztbriefe. Die Daten können sowohl durch Leistungserbringer als auch durch den Patienten selbst in die Akte geschrieben werden.

1.2 Vertraulichkeit

Ausschluss unbefugter Kenntnisnahme durch Verschlüsselung

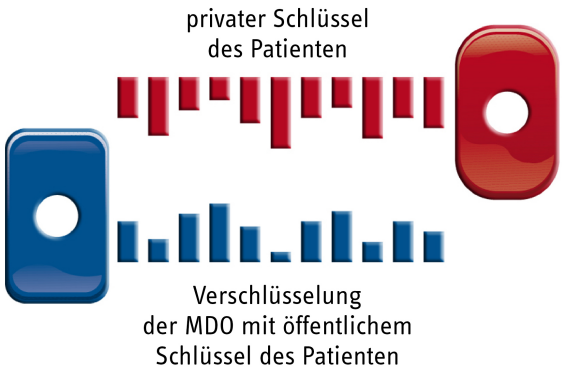
Die unbefugte Kenntnisnahme von MDOs und das Erschließen von Informationen ist durch das Datenschutzsystem von CGM LIFE ausgeschlossen. Grundlage hierfür ist eine patienten-individuelle Verschlüsselung der Daten vor der Übertragung an und Speicherung auf die CGM LIFE Server.

Die Zugangsschlüssel liegen ausschließlich in der Kontrolle des Patienten selbst. Eine eigenmächtige Entschlüsselung der Daten durch den Betreiber darf technisch nicht möglich sein.

Der Patient alleine besitzt die Schlüsselgewalt

Dieses Prinzip wird erreicht durch die kryptographische Verschlüsselung aller medizinischen Daten auf dem Rechner des Anwenders. Dies gilt sowohl für den Rechner des Patienten, der selbst Daten in seine Akte einstellt, als auch für Leistungserbringer, die Daten in die elektronische Patientenakte einstellen oder aus ihr abrufen.

Nur der Patient hat Zugriff auf den privaten Schlüssel



Zugriff von zuhause

Der Patient kann selbständig von zuhause über ein entsprechendes Programm auf seine Akte zugreifen. Dieses Programm läuft in jedem aktuellen Webbrowser und ist einfach über das Internet aufrufbar.

Zugriff über

Der Patient authentifiziert sich selbst durch Eingabe eines Benutzernamen und eines Passworts. Aus dem Passwort des Benutzers

Benutzername/Passwort

wird in diesem Fall der kryptographische Schlüssel abgeleitet, der zur Entschlüsselung der medizinischen Daten notwendig ist. Weder das Passwort noch ein Abbild des Passworts wird zu irgendeinem Zeitpunkt an den Server übertragen.

Zur Erhöhung der Sicherheit kann Zwei-Faktor-Authentifizierung mithilfe mobile TAN (MTAN) oder Time-based-One-Time-Password (TOTP) eingesetzt werden.

Keine Hintertüren

CGM kann die Verschlüsselung der Daten nicht umgehen. Dementsprechend kann CGM das Passwort eines Benutzers nicht eigenmächtig zurücksetzen. Denn um dies zu tun, müsste der Betreiber Zugriff auf die Schlüssel des Patienten haben, was per Design ausgeschlossen ist.

Zweitschlüssel bei Passwortverlust

Für den Fall, dass der Patient sein Zugangspasswort verliert, kann sich der Patient daher selber Zweitschlüssel, die „SuperPIN“, ausstellen, die er selbst sicher aufbewahrt oder zur Aufbewahrung an einen Dritten, z.B. den Arzt seines Vertrauens, weitergeben kann. Bei Verlust des Passworts kann der Patient so den Zugriff auf seine Akte wiederherstellen.

Keine zentrale Instanz zur Speicherung von Zweitschlüsseln

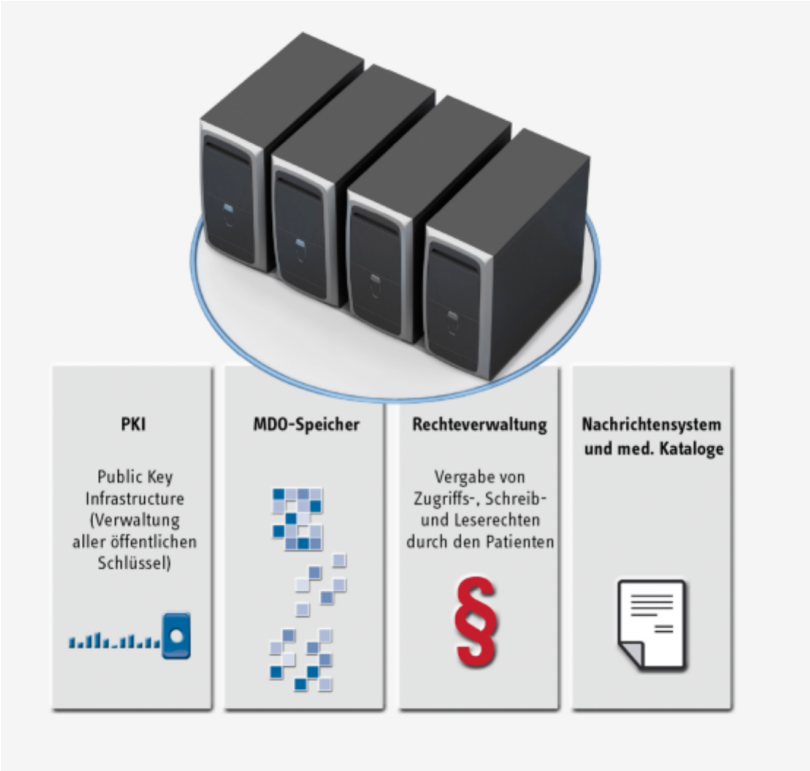
Durch den Verzicht auf eine Zentralinstanz zur Speicherung von Zweitschlüsseln wird verhindert, dass Spione oder Diebe an einer einzigen Stelle gezielt Zugriff auf Patientenakten erbeuten können.

1.3 Berechtigungsmanagement

Der Patient gewährt Dritten Zugriff auf seine Akte

Der Patient hat die Möglichkeit, Dritte für den Zugriff auf seine Patientenakte zu ermächtigen. Hierzu stellt er auf digitalem Weg einen zweiten Zugangsschlüssel zu seiner Akte einem Dritten zur Verfügung, der hiermit auf die Akte zugreifen und die darin enthaltenen Daten entschlüsseln kann. Der Patient hat jederzeit das Recht und die Möglichkeit, Dritten den gewährten Zugriff wieder zu entziehen.

Ende-zu-Ende Verschlüsselung mit Hilfe der PKI



Bevollmächtigung

Darüber hinaus kann der Patient Dritte zur Führung seiner Akte bevollmächtigen. So können z.B. Kinder die Akte Ihrer pflegebedürftigen Eltern in deren Auftrag führen, sowie Eltern die Akte ihrer minderjährigen Kinder.

Zur Verwaltung der kryptographischen Schlüssel beinhaltet CGM LIFE eine Public Key Infrastructure (PKI), die die öffentlichen Schlüssel aller Beteiligten verwaltet und ermöglicht, verschlüsselte Nachrichten und medizinische Daten zwischen den Beteiligten auszutauschen, ohne dass CGM die Daten mitlesen kann.

1.4 Integrität und Authentizität

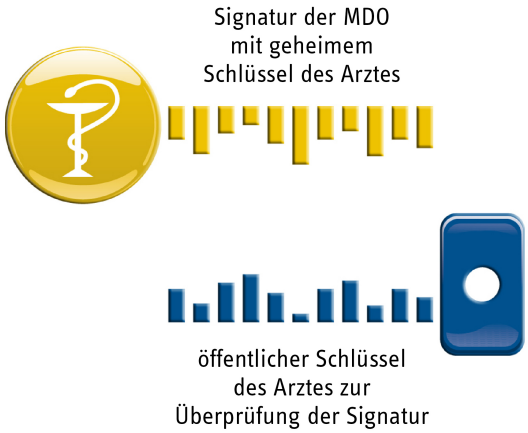
Unversehrtheit medizinischer Daten

CGM LIFE garantiert die Unversehrtheit und Echtheit aller gespeicherten Daten. Dies wird erreicht durch digitale Signaturen, die für jeden Eintrag der Akte erstellt erstellt werden.

- Das lokale Arzt- oder Klinik-Informationssystem stellt die medizinischen Informationen als Kopie in die elektronische Patientenakte. Jeder Eintrag ist vom Autor mit seinem persönlichen Schlüssel digital signiert. Der Autor bestätigt somit den von ihm eingestellten Inhalt.

- Änderungen, z.B. Korrekturen, kann nur der Autor vornehmen! **Autorenprinzip**
- Alle Änderungen werden protokolliert.
- Modifikation durch Dritte ist technisch ausgeschlossen.

Schutz vor unbefugter Modifikation durch digitale Signaturen



Alle an die elektronische Patientenakte übertragenen Daten können damit eindeutig und nachweisbar dem Autor zugeordnet werden.

Identifikation der Teilnehmer über die PKI

1.5 Verfügbarkeit

CGM LIFE speichert alle Daten auf zentralen Cloud-Servern ab, um eine ununterbrochene Verfügbarkeit der Daten im 24-Stundenbetrieb an 7 Tagen in der Woche zu gewährleisten.

Schutz vor unvorhersehbaren Ausfällen

Die CGM LIFE Server werden in Deutschland betrieben.

1.6 Revisionsfähigkeit

Alle Änderungen an den gespeicherten medizinischen Daten werden in Protokolldaten festgehalten. So sind Datenänderungen und Datenlöschungen für den Patienten und die durch ihn berechtigten Leistungserbringer jederzeit nachvollziehbar.

Alle Transaktionen werden protokolliert