MATERNA
Virtual Solution

Sichere mobile Kommunikation im Krankenhaus

Materna Virtual Solution GmbH · Januar 2023

MATERNA
Virtual Solution

Inhalt

Seite

MATERNA
Virtual Solution

Eine interdisziplinäre und standortübergreifende Zusammenarbeit zwischen Kolleg:innen

Soziale Netzwerke und Messenger-Dienste spielen im Alltag eine immer bedeutendere Rolle. Sie ermöglichen nie den schnellen und unkomplizierten Austausch von Nachrichten zwischen Personen und Personengruppen. Zunehmend werden solche Dienste jedoch auch im Business-Umfeld zur Übermittlung persönlicher sensibler Daten genutzt. Die Gewissheit einer Ende-zu-Ende-Verschlüsselung mag hier treibend für eine gefühlte Sicherheit in der Datenübermittlung sein. Problematisch wird die Nutzung jedoch, wenn sie auf schützenswerte Daten Dritter ausgeweitet wird: Das Versenden elektronischer Patient:innendaten z.B. über WhatsApp ist nicht nur nicht wünschenswert, sondern erfolgt zudem nicht unter den geltenden regulativen Anforderungen, wie sie etwa die Datenschutz-Grundverordnung (DSGVO) fordert. Gleichzeitig macht es die fortschreitende Digitalisierung auch im Gesundheitswesen erforderlich, intersektorale Kommunikations- und Nachrichtenplattformen sowie Messenger-Dienste einzuführen.[1]

Der Einsatz von Messenger-Diensten in Gesundheitseinrichtungen ist vielfältig. Die krankenhausinterne Kommunikation z.B. im Kontext eines Konsils aber auch die Kommunikation mit Externen wie niedergelassenen Ärzt:innen als Zu- und Einweiser, Mitgliedern intersektoraler Versorgung, beispielsweise im Rahmen von Tumorboards oder die Kommunikation mit anderen Leistungserbringer:innen wie Rettungsdiensten, Alten- und Pflegeheimen, Reha-Kliniken oder externen Therapeut:innen, sind nur einige Szenarien, bei denen ein schneller und unkomplizierter Informationsaustausch unabdingbar ist. Auch die digitale Kommunikation mit Patient:innen und Angehörigen rückt zunehmend in den Fokus der Leistungserbringer:innen. Je nach Anwendungsbereich ergeben sich dabei unterschiedliche Anforderungen an die entsprechende digitale Kommunikationslösung.

Insbesondere der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliegt gesetzlichen Daten-

1 § 22 BDSG besagt, : die Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig, wenn sie zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder [...].

schutzvorgaben, denen gängige Messenger-Dienste wie WhatsApp bislang nicht oder nur bedingt entsprechen. Für einen professionellen Einsatz im Krankenhaus kommen sie daher nicht in Frage. Mit Blick auf die Sensibilität der im Gesundheitsbereich geführten Daten und der hohen Schutzbedürftigkeit, den diese nach Art. 9 DSGVO[2] genießen, sind daher bei der Auswahl geeigneter Informationsdienste- für die Übermittlung von Patient:innendaten im Krankenhausbereich von den Verantwortlichen umfangreiche Datenschutzanforderungen zu berücksichtigen.

Zum Beispiel muss verhindert werden, dass übermittelte Bilddaten automatisch in einer beliebigen Cloud-Umgebung gespeichert werden. Ebenso ist sicherzustellen, dass Daten nicht versehentlich an eine falsche Person geschickt werden: kommerzielle Messenger-Dienste interagieren mit beliebigen Kontaktlisten, und aus diesen können fälschlicherweise ungeeignete Adressaten ausgewählt werden. Allein schon die Benutzung von WhatsApp verletzt bei Zugriff auf das Adressbuch die Persönlichkeitsrechte der Kontakte, die nicht in eine Übermittlung ihrer Daten an WhatsApp eingewilligt haben. Die Übermittlung personenbezogener Gesundheitsdaten über WhatsApp ist strafbewehrt. Im Adressbuch können zudem Daten von Kolleg:innen gespeichert sein, wodurch eine Kompromittierung stattfindet und der Arbeitsschutz nicht gewährleistet ist. Hier drohen ebenfalls Sanktionen.

Die Kommunikation zwischen dem medizinischen Fachpersonal und anderen Berufsgruppen wird bisher primär über Telefon, Fax oder das persönliche Gespräch abgebildet, kommerzielle Messenger-Dienste kommen ebenfalls zum Einsatz.

Eine repräsentative Umfrage des Deutschen Datenschutz-Instituts (DDI) zeigt, dass in Deutschland 98 Prozent der Klinikärzt:innen Messenger-Dienste nutzen. Zwei Drittel der Klinikärzt:innen halten sie auch im Krankenhausalltag für sinnvoll, und 54 Prozent nutzen sie aktiv zur Befundübermittlung. Die Mehrheit ist der Auffassung, dass durch die rasche und unkomplizierte Befundübermittlung die Versorgung der Patient:innen verbessert wird[3].

Als weiteres Ergebnis der DDI-Umfrage gaben 66 Prozent der befragten Ärzt:innen jedoch an, dass sie ihren Messenger für unsicher halten, und 84 Prozent sagten, dass sie Patient:inneninformationen auf Fotos vor Übermittlung unkenntlich machen. Solche manuellen Versuche, Daten zu anonymisieren, sind jedoch zumeist unwirksam.[3]

98 %
der Klinikärzt:innen nutzen **MESSENGERDIENSTE.**[3]

54 %
nutzen sie aktiv zur **BEFUNDÜBERMITTLUNG.**[3]

66 %
der befragten Ärzt:innen geben jedoch an, dass sie **IHREN MESSENGER FÜR UNSICHER** halten.[3]

2 Gem. Art. 9 Abs. 1 DSGVO sind u.a. Gesundheitsdaten eine besondere Kategorie personenbezogener Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person (Patienten), einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

3 https://deutsches-datenschutz-institut.de/wp-content/uploads/2021/05/FAZ_Messenger-2018.pdf

MATERNA Virtual Solution

Die Herausforderung: Datenschutzkonforme Kommunikation mit sensiblen Daten

Aufgrund des hohen Risikos einer Datenschutzverletzung wird eine Alternative zu kommerziellen Nachrichtendiensten benötigt, die für einen Einsatz im Gesundheitswesen in Frage kommen darf. Medizinische Einrichtungen sollten bemüht sein, ihren Mitarbeitenden sichere Kommunikationsmöglichkeiten zur Verfügung zu stellen. Gleichzeitig sollten Ärzt:innen sich nicht dazu verleiten lassen, unsichere Messenger beruflich nur deswegen zu nutzen, weil es keine sicheren Alternativen gibt und eine Strafverfolgung eher selten ist. Die Nutzung nicht datenschutzkonformer Kommunikationslösungen macht gemäß DSGVO Entscheider:innen auch persönlich haftbar.

Wann liegt ein Verstoß gegen die DSGVO vor?

Gemäß DSGVO ist **jede unrechtmäßige Nutzung persönlicher Daten gesetzeswidrig**. Es ist irrelevant, ob diese Daten genutzt oder nur zu Statistikzwecken erhoben und zwischengespeichert werden – Unternehmen sind verpflichtet, jede mögliche Nutzung anzugeben und eine schriftliche Genehmigung des jeweiligen Nutzenden einzuholen.

Die DSGVO gilt nicht nur für Unternehmen, sondern auch für Privatpersonen, die fremde Daten verarbeiten – z. B. auf einem persönlichen Blog mit Newsletter. Eine Ausnahme bilden rein private Seiten, die ohne Nutzung jeglicher Kontaktdaten auskommen.

MATERNA
Virtual Solution

Unsere Lösung: Sichere mobile Kommunikation im Gesundheitswesen mit SecurePIM

SecurePIM, die Systemlösung für ultramobiles Arbeiten, bündelt alle wichtigen Business-Funktionen wie E-Mail, Messenger, Sprach- und Videotelefonie, Kontakte, Kalender, Notizen, Aufgaben, Dokumente und vieles mehr sicher in einer App. Dank innovativer Containertechnologie und der vom BSI geprüften Sicherheitsarchitektur können sensible Daten geräteunabhängig und plattformübergreifend versendet und gespeichert werden.

Der Zugang zum Internet und Intranet befindet sich in einem gesicherten Bereich auf dem Smartphone oder Tablet (iOS und Android). Dadurch können Inhalte aus E-Mails und Dokumenten im Chat geteilt werden, ohne die Anwendung verlassen zu müssen. Das ist zum einen ein großer Sicherheitsvorteil, zum anderen auch sehr komfortabel. Und durch die nahtlose Integration des Messengers behalten Sie immer die volle Kontrolle über dienstliche Daten. Dank der engen Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet SecurePIM höchste Sicherheit bei mobiler Kommunikation.

Der integrierte Messenger von SecurePIM

Mit dem integrierten Messenger in SecurePIM können Beschäftigte des Gesundheitswesens sicher und DSGVO-konform miteinander kommunizieren – in Gruppen oder One-to-One. Funktionen des Messengers umfassen u. a. das verschlüsselte Telefonieren auch mit Videoübertragung, das einfache Versenden von Dokumenten und Bildern, das Übertragen von Live-Standorten sowie das Kommunizieren über Channels mit bis zu 255 Nutzer:innen.

Durch die Container-Technologie von SecurePIM können die Mitarbeitenden ihre eigenen Mobilgeräte (iOS und Android) für die sichere und DSGVO-konforme Kommunikation von geschützten Patient:innendaten nutzen. Somit lassen sich Bring-Your-Own-Device-Konzepte (BYOD) schnell und sicher realisieren.

Der integrierte Messenger von SecurePIM – die Vorteile:

+ Einfache & schnelle Kommunikation: Vom One-To-One-Chat über Channels für 255 Personen bis zur verschlüsselten Video-Telefonie.
+ Bring-Your-Own-Device-Nutzung der eigenen Mobilgeräte (iOS und Android)
+ Einfache Installation und Benutzermanagement– zentrale Verwaltung
+ Alle Kernkomponenten und die Sicherheitsarchitektur sind vom deutschen Hersteller in Deutschland entwickelt.
+ Out-Of-The-Box DSGVO-konformes Messaging.
+ Intuitive Nutzung. Schneller Start. Kein Schulungsaufwand.
+ Maximale Sicherheit: Verwendet die eigenentwickelte und vom BSI geprüfte Sicherheitsarchitektur SERA.
+ Der Messenger ist als Stand-Alone-App SecureCOM oder vollintegriert in SecurePIM verfügbar.

MATERNA
Virtual Solution

SecureCOM – der-Stand-Alone-Messenger für den Gesundheitsmarkt

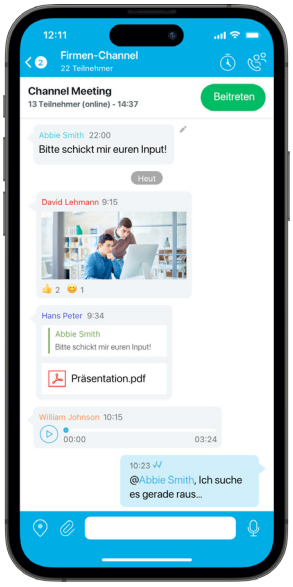
SecureCOM ist die Stand-Alone-Variante des in SecurePIM integrierten Messengers und beinhaltet die gleichen Funktionen. Mit der App SecureCOM können Ihre Mitarbeitenden bequem, sicher und DSGVO-konform kommunizieren – einzeln mit ihren Kontakten oder in Gruppen. Der Messenger bietet verschlüsselte Telefonie mit und ohne Videoübertragung, den Austausch von Dokumenten und Bildern sowie spezifische Funktionen für den Gesundheitsmarkt, wie z.B. erweiterte Standortfunktionen für Einsatzkräfte (Notarzt, Rettungsdienst, etc.). Die intuitive Bedienoberfläche sorgt dafür, dass sich Mitarbeitende sofort zurechtfinden und keine zusätzlichen Schulungen benötigen.

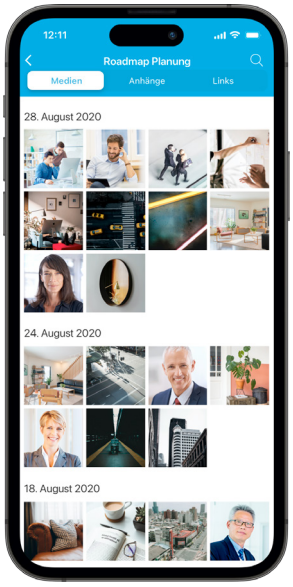
Einfache Implementierung, Konfiguration und Rollout

Der Messenger, als Stand-Alone-Variante SecureCOM oder integriert in SecurePIM, lässt sich schnell in jede bestehende IT-Infrastruktur integrieren. Alle notwendigen Komponenten kommen aus einer Hand. Wenn SecurePIM bereits im Einsatz ist, kann der Messenger durch ein einfaches Upgrade hinzugefügt werden. Für die Implementierung und den Betrieb sind alle nötigen Schritte und Komponenten detailliert und auf Deutsch dokumentiert. Administrator:innen verwalten zentral über das SecurePIM Management Portal alle Endgeräte und Accounts. Der Rollout der App geht schnell und einfach. Mitarbeitende laden sich die App aus dem Apple® App Store oder GooglePlayTM herunter und melden sich mit ihren Zugangsdaten an. Alternativ kann SecureCOM auch über ein Mobile-Device-Management-System oder interne App Stores ausgerollt und gesteuert werden. Secure by Design SecureCOM verfügt über ein komponentenübergreifendes Sicherheitskonzept. Alle Dienste sind innerhalb der Plattformgrenzen sicher eingeschlossen. Das Systemdesign ist vollständig darauf ausgelegt, dass keinerlei Daten an externe oder öffentliche Dienste weitergegeben werden. Andere Apps auf dem Gerät oder unautorisierte Personen können nicht auf die Daten in SecureCOM zugreifen. Im Rahmen eines BYOD-Ansatzes kann damit z.B. WhatsApp aus dem dienstlichen Bereich verbannt – privat aber weiterhin genutzt werden.

MATERNA Virtual Solution

SecureCOM-Funktionen



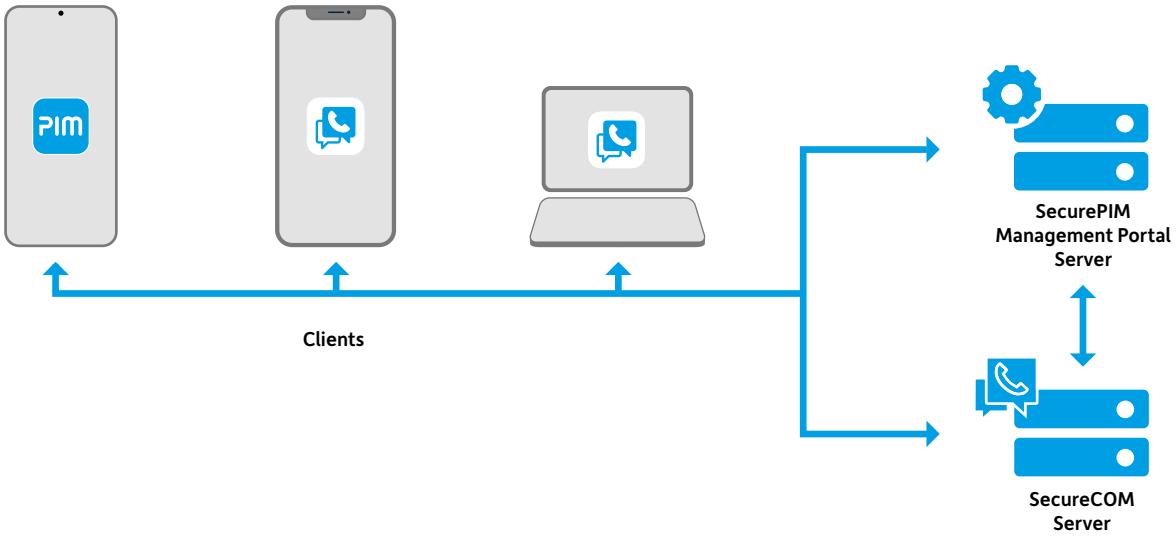


Funktionsübersicht

- One-to-One-und Gruppen-Chats
- Channels für spezifische Themen
- Vollbildmodus für Präsentationen
- Bilder und Dokumente versenden oder teilen
- Sprachnachrichten versenden
- Standortmarkierungen und Live-Standort teilen
- Bildschirm teilen (Desktop- und Android-Version)
- Audio- und Video-Anrufe + Audio- und Video-Konferenzen Kompatibilität
- Als App plattformübergreifend und geräteunabhängig für iOS und Android, als DesktopVersion für Windows, macOS und Linux
- Synchronisation mit Active Directory oder LDAP
- SecureCOM ist als Stand-Alone-App oder vollintegriert in SecurePIM verfügbar

MATERNA
Virtual Solution

SecureCOM-Komponenten



Sicherheit

+ Nachrichten werden Ende-zu-Ende verschlüsselt versendet
+ Alle Nachrichten, Kontakte, private Schlüssel und PINs werden nach höchsten Sicherheitsstandards verschlüsselt
+ Verwendung von Verschlüsselungs- und Hash-Algorithmen, die vom BSI evaluiert und akkreditiert wurden
+ Es werden keinerlei persönliche Daten auf dem Server gespeichert
+ Der SecureCOM-Server ist als Cloud-Lösung oder On-Premises verfügbar

MATERNA
Virtual Solution

Über Materna Virtual Solution

Materna Virtual Solution, ein Unternehmen der Materna-Gruppe, ist ein auf sichere mobile Anwendungen spezialisierter Softwarehersteller mit Sitz in München und Entwicklungsstandort in Berlin.

Das Unternehmen entwickelt und vertreibt die Applikationen SecurePIM, SecureCOM und die Sicherheitsarchitektur SERA für iOS und Android. SecurePIM ermöglicht verschlüsseltes und benutzerfreundliches mobiles Arbeiten. Behörden können mit Smartphones und Tablets auf Geheimhaltungsstufe VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) und auf der Sicherheitsstufe NATO RESTRICTED kommunizieren.

Für Unternehmen stellt SecurePIM die Anforderungen der Datenschutzgrundverordnung (DSGVO) auf mobilen Geräten sicher und senkt damit die Risiken strafbewährter DSGVO-Verstöße und des Verlustes von Unternehmensdaten.

Materna Virtual Solution wurde 1996 gegründet und beschäftigt rund 100 Mitarbeiter:innen. Alle Produkte der Materna Virtual Solution tragen das Vertrauenszeichen »IT-Security made in Germany« des TeleTrust-IT-Bundesverbandes IT-Sicherheit e.V.

Sprechen Sie mit uns!

kontakt@virtual-solution.com
T +49 89 30 90 57-0

P-23.0023_Whitepaper_Gesundheitswesen_de/de_v2_01/23

MATERNA
Virtual Solution

Materna Virtual Solution GmbH
Blutenburgstraße 18 · 80636 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com