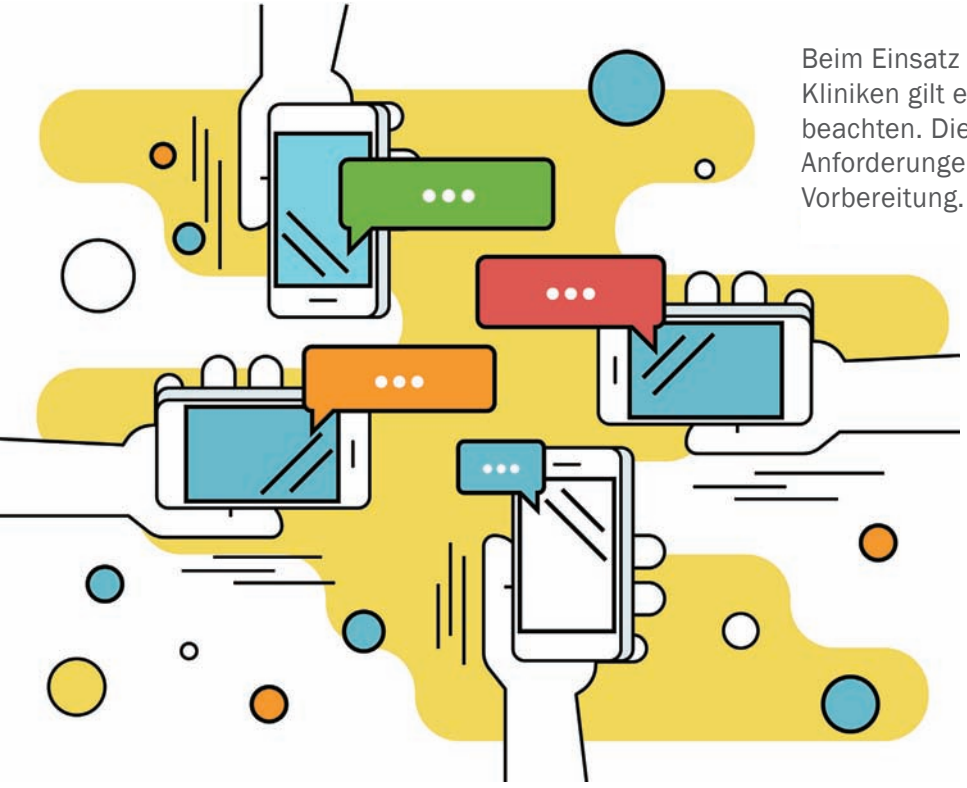
ARBEITSORGANISATION

Instant-Messengerdienste: Wo die Fallstricke lauern



Beim Einsatz von Instant-Messengerdiensten in Kliniken gilt es, einiges in Sachen Datenschutz zu beachten. Die technischen und organisatorischen Anforderungen sind hoch und erfordern Zeit der Vorbereitung.

Eine kurzfristig umsetzbare und unkomplizierte Kommunikation ist gerade im Krisenfall unerlässlich. Aber auch die barrierefreie Kommunikation mit Patienten und niedergelassenen Ärztinnen und Ärzten gewinnt an Bedeutung. Der Einsatz von Instant-Messengerdiensten kann dabei helfen. Doch viele der im Privatleben gängigen Dienste sind in puncto Datenschutz und Datensicherheit nicht für den klinischen Kontext geeignet. Daher hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ein Whitepaper veröffentlicht, das die technischen Datenschutzanforderungen an Instant-Messengerdienste im Krankenhaus definiert.

Muss-Anforderungen des DSK-Whitepapers

Das Whitepaper nennt vier Maßnahmenbereiche zu den Themen Messengerapplikation, Kommunikation, Sicherheit der Endgeräte sowie Plattform/Betrieb des Messengerdienstes. Da das Whitepaper Richtliniencharakter hat, sollten Kliniken keinen Messenger zur Verarbeitung patientenbezogener Daten nutzen, der nicht alle Muss-Kriterien erfüllt. Folgende Muss-Anforderungen hat die DSK definiert:

- Die Nutzer werden über die Datenverarbeitung informiert.
- Der Zugriff auf den Messengerdienst ist durch ein vorheriges Authentifizierungsverfahren gesichert, das über eine reine Entsperrung des Mobilgeräts hinausgeht.
- Die Kontaktdaten innerhalb des Messengerdienstes sind vom allgemeinen Adressbuch getrennt.
- Nachrichten und Dateianhänge werden in einem vom allgemeinen Speicher separaten Bereich verschlüsselt gespeichert.
- Bei der Nutzung von elektronischen Zertifikaten liegt ein Zertifikatsmanager vor.
- Daten, die durch die Applikation verwaltet werden, können gelöscht werden.
- Eine initiale Datenübermittlung an Dienste Dritter zum Zweck der Fehleranalyse bedarf der Zustimmung des Nutzers.
- Datenkategorien werden benannt, die für eine Fehleranalyse übertragen werden; dabei handelt es sich nicht um Daten zum Nutzungsverhalten und Daten, die dem Arztgeheimnis unterliegen.
- Es gibt eine Möglichkeit, Daten ins Krankenhausinformationssystem zu übertragen.
- Werden Daten bei einem Dienstleister, zum Beispiel in einer Cloud, gesichert, werden die Daten verschlüsselt abgelegt und transportiert.
- Bei der Applikation ist der Grundsatz Privacy by Default umgesetzt.
- Die Kommunikation erfolgt über eine Ende-zu-Ende-Verschlüsselung.
- Es kann nachvollzogen werden, ob der Empfänger die Nachricht/Daten erhalten hat.
- Der Speicherort der Applikation auf dem Mobilgerät liegt verschlüsselt vor.
- Innerhalb des Registrierungsprozesses wird eine Identitätsfeststellung des Nutzers vorgenommen.

Technische und organisatorische Voraussetzung

Zudem sind Maßnahmen umzusetzen, die sich aus den Anforderungen der Datenschutzgesetze ergeben. Da die meisten Messenger über externe Dienstleister bezogen werden, sollten Kliniken zwingend einen Vertrag zur Auftragsdatenverarbeitung abschließen. Dabei gilt es, die bereichsspezifischen Vorschriften zu beachten. Die Landeskrankenhausgesetze in Bayern und Baden-Württemberg definieren beispielsweise besondere

Foto: Julia Tim/stock.adobe.com

Voraussetzungen für die Auftragsverarbeitung oder schließen diese gar aus. Um den Einsatz rechtskonform zu gewährleisten, müssten die Messenger im Rechenzentrum der Klinik betrieben werden.

Vor der ersten Anwendung des Messengerdienstes müssen Kliniken eine dokumentierte Datenschutzfolgenabschätzung vornehmen. Wichtig ist, die Einsatzzwecke bereits exakt festgelegt zu haben. In Abhängigkeit davon, ob eine Klinik den Messenger nur für die krankenhausinterne Nutzung, fachliche Konsile, die Kommunikation mit Rettungsdiensten, Arztpraxen und anderen Leistungserbringern oder für die Kommunikation mit Patienten nutzen will, verändert sich die Einschätzung der möglichen Risiken und in der Folge auch die Notwendigkeit, eine Datenschutzfolgenabschätzung vorzunehmen. Ferner ist darauf zu achten, dass das Messengerdienst-System nur als Unterstützungssystem verwendet wird und niemals das Krankenhausinformationssystem ersetzt. Außerdem müssen Kliniken eine Nutzungsrichtlinie erarbeiten, damit alle Anwender wissen, zu welchen Zwecken der Messengerdienst zugelassen ist, welche Schutzmaßnahmen sie zu beachten und wie sie im Falle einer Datenschutzverletzung vorzugehen haben.

Hürde Datenverarbeitung in den USA

Seit dem Wegfall des Privacy Shields durch ein Urteil des Europäischen Gerichtshofs ist die Datenverarbeitung in den USA problematisch (Urteil vom 16. Juli 2020, Rechtssache C-311/18). Dabei geht es um das Risiko, dass US-Geheimdienste Zugriff auf die sensiblen Daten nehmen könnten. Sorgfältig zu prüfen ist, ob ein Messengerdienst Daten in den USA verarbeitet und welche Maßnahmen zum Schutz dieser ergriffen wurden. Das gilt auch für etwaige Unterauftragnehmer, wie Amazon Web Services.

Zudem ist zu prüfen, ob weitere, für das Krankenhaus relevante Vorschriften zu beachten sind. Die Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche beispielsweise verlangt neben der Datenverarbeitung im Europäischen Wirtschaftsraum auch zwingend eine Punkt-zu-Punkt-Verschlüsselung.

Messenger: keine private Nutzung

Kliniken sollten schon in der Planungsphase den Betriebsrat einbinden und, falls erforderlich, eine Betriebsvereinbarung abschließen. Darin sollte die private Nutzung des dienstlichen Messengers ausgeschlossen werden. Zum einen begründet sich das aus den Anforderungen des Telekommunikationsgesetzes und der damit verbundenen Störerhaftung. Zum anderen würde die private Nutzung mögliche Kontrollerfordernisse im Falle eines Datenschutzvorfalls erschweren. Der Ausschluss der privaten Nutzung schließt jedoch nicht aus, den Messenger auf einem privaten Endgerät zu installieren, wenn Kliniken über eine sogenannte Bring-Your-Own-Device-Regelung verfügen. Dann müssen die Mobilgeräte über ein Mobile-Device-Management-System administriert und konfiguriert werden. Dies ist wichtig, um im Verlustfall eine Rücksetzung zu gewährleisten sowie die Installation von Sicherheitspatches und Aktualisierungen. Auch muss verhindert werden, dass die Anwender den Zugriffsschutz, wie PIN/Passphrase, eigenmächtig umgehen oder ausstellen können.

David Große Dütting, Seniorberater Datenschutz
Marco Eck, Berater Datenschutz
Curacon GmbH
Wirtschaftsprüfungsgesellschaft
48155 Münster

KARRIERE KONKRET

„Man muss Medizinisches auch mal delegieren können“

Herr Prof. Kausch von Schmeling, was braucht es neben der fachlichen Leistung, um Chefarzt zu werden?
Entscheidend ist für mich die Freude, im Team zu arbeiten. Ich führe täglich Gespräche mit Mitarbeitenden und muss dabei meist Probleme lösen. Das macht nur Spaß, wenn man ernsthaftes Interesse hat, für das Team da zu sein. Wichtig zu wissen ist auch, dass man als Chef immer vorne steht, also ausgesprochen exponiert ist. Das sollte einem schon zusagen. Auch sind Geduld und Diplomatie wertvolle Eigenschaften, die man manchmal erst erlernen muss.

Wie gelingt Ihnen der Spagat zwischen Medizin und Management?
Gerade das macht ja Spaß. Um ausreichend Zeit für das Management zu haben, muss man Medizinisches auch mal delegieren können. Das ist mitunter gar nicht einfach. Erstens muss man lernen, anderen Aufträge zu erteilen. Zweitens möchte man vieles ja auch gerne selbst machen.

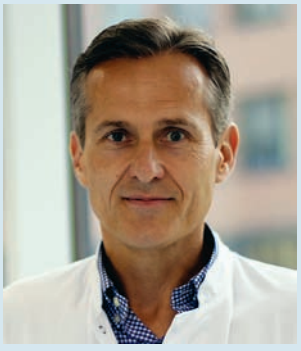


Foto: Ammerland-Klinik GmbH

Interview mit Prof. Dr. med. Ingo Kausch von Schmeling, Chefarzt der Klinik für Urologie und Kinderurologie und Leiter des zertifizierten Prostatazentrums an der Ammerland-Klinik in Westerstede

Was ist die größte, nicht fachliche Herausforderung?
Das sind die täglichen Frustrationen, zum Beispiel morgens als Erstes zu hören, dass zwei Mitarbeitende krank sind und ein OP-Saal wegen technischer Probleme nicht läuft. Doch auch das gehört dazu.

Warum interessieren sich immer weniger Ärztinnen und Ärzte für eine Karriere im Krankenhaus?
Eine Karriere bedeutet heute deutlich mehr Verantwortung und die Bezahlung, zum Beispiel der Chefärzte, ist bei Weitem nicht mehr so hoch wie vor 20 oder 30 Jahren.

Was raten Sie jungen Ärztinnen und Ärzten, die nach oben wollen?
Sie sollten so viel lernen wie möglich. Ich empfehle als Zusatzqualifikation immer eine Promotion. Zudem ist es wichtig, in Zielvereinbarungs- und Evaluationsgesprächen eigene Wünsche klar zum Ausdruck zu bringen. ***sg***