Digitale Kommunikation im Gesundheitswesen

Die „schöne neue digitale Welt“ eröffnet uns viele Möglichkeiten, schneller und unkomplizierter miteinander zu kommunizieren. Doch welche Websites sind wirklich sicher und welche Tücken haben Messenger-Dienste wie WhatsApp und Co.? Dies und mehr lesen Sie in diesem Fachbeitrag von Dr. Christine Trutt-Ibing.

Würden Sie Ihre Bankverbindung oder Ihre Zugangsdaten zu einem Online-Shop auf eine Postkarte schreiben und per Post verschicken? Wahrscheinlich nicht, denn schließlich handelt es sich um vertrauliche Daten, die nicht von jedem gelesen werden sollen. Sie würden solche Daten wohl eher in einem verschlossenen Briefumschlag verschicken.

SSL-SICHERHEITSZERTIFIKATE

Und im Internet? Hier hat die Funktion des Briefumschlages ein sogenanntes SSL-Verschlüsselungs-Zertifikat auf dem Webserver. In der Adressleiste des Browsers steht dann „https“ statt „http“ und die Browser zeigen in der Regel auch das Symbol eines kleinen Schlosses in der Adressleiste an. Websitebetreiber, die Formulare (zum Beispiel Kontaktformulare oder Formulare zum Einloggen oder Anmelden et cetera) auf ihren Websites anbieten, sind gesetzlich verpflichtet, die eingegebenen Daten ihrer Besucher beim Transport über das Internet zu schützen.

Viele Arztpraxen verfügen über eine Praxishomepage mit einem Kontaktformular oder Formularen zur Bestellung von Rezepten und Überweisungen. Auch hier muss die Website über ein solches Sicherheitszertifikat verfügen. Wer als Betreiber einer Praxiswebsite solche Formulare nicht verwendet, braucht nicht zwingend ein solches Zertifikat. Jedoch gehört es im Internet inzwischen zum guten Ton, solche Zertifikate zu verwenden. Viele Browser geben sogar eine Warnmeldung aus, wenn auf einer Website kein SSL-Zertifikat vorhanden ist, und klassifizieren diese als „nicht sicher“. Und das macht natürlich keinen guten Eindruck. Einfache Sicherheitszertifikate sind nicht teuer. Manche Provider bieten sie in ihren Webhosting-Paketen sogar kostenlos an. Sie müssen dann nur aktiviert werden. Leider gaukeln solche SSL-Zertifikate eine falsche Sicherheit vor, da sie implizieren, dass von einer Website keine Gefahr ausgeht. Das ist jedoch nicht der Fall. Auch auf einer vermeintlich sicheren Seite kann Schadcode lauern.

SICHERER AUSTAUSCH/KOMMUNIKATION MIT KOLLEGEN

E-Mail

E-Mail ist (noch) die am weitesten verbreitete digitale Kommunikationsform. Fast jeder Bundesbürger hat eine E-Mail-Adresse. Doch leider ist die Kommunikation per E-Mail nicht sicher genug ist, um vertrauliche Informationen auszutauschen!

Nun gibt es auch bei E-Mails die Möglichkeit, diese sozusagen in Geheimschrift zu verfassen, die nur vom Empfänger gelesen werden kann. Man spricht im Fachjargon von einer Ende-zu-Ende-Verschlüsselung. Diese ist für Laien relativ kompliziert einzurichten und deshalb wird sie kaum genutzt.

Aber für die Praxen ist eine Lösung in Sicht. Sie heißt KIM.

KIM (Kommunikation im Medizinwesen)

Bei KIM handelt sich um einen E-Mail-Dienst, der nur innerhalb der sich im Aufbau befindenden Telematik-Infrastruktur zum Einsatz kommt. Über KIM können zukünftig alle Nachrichten, Befunde und Arztbriefe sicher verschickt werden. Dabei wird der E-Mail-Dienst

direkt an das Praxis- oder Klinikverwaltungssystem angebunden. So können eingehende Befunde gleich in der digitalen Akte eines Patienten gespeichert werden. Und auch die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) soll zukünftig über KIM an die Krankenkassen verschickt werden.

Die Telematik-Infrastruktur **verbindet nur Akteure des Gesundheitswesens**, also Ärzte, Krankenhäuser, Apotheken und Krankenkassen, später vielleicht noch Physiotherapeuten, Hebammen, Logopäden etc. Fraglich ist jedoch, ob letztere Berufsgruppen den finanziellen und technischen Aufwand überhaupt stemmen können. Ein Austausch von Dokumenten mit Patienten ist über KIM nicht möglich. Hier wird jedoch die elektronische Patientenakte (ePA) neue Möglichkeiten schaffen.

Infobox

Die KV Hessen hat ihren Mitgliedern Anfang Februar eine ausführliche Broschüre mit Informationen zu KIM zugesandt. Die aktuelle Fassung der Broschüre finden Sie unter
www.kvhessen.de/publikationen/kim-dienst

Messenger-Apps

Seit dem Siegeszug der Smartphones erfreuen sich Messenger-Apps einer immer größeren Beliebtheit. Im Ranking der Messenger-Apps steht WhatsApp unangefochten an der Spitze. Der zum Facebook-Konzern gehörende Messenger-Dienst findet sich auf fast jedem Privathandy. Was liegt da näher, als ihn auch im beruflichen Umfeld zu nutzen und mal eben schnell mit einem Kollegen Befunde auszutauschen oder eine berufliche Meinung einzuholen?

Inzwischen hat sich herumgesprochen, dass WhatsApp im beruflichen Umfeld ein No-Go ist, da WhatsApp Nutzerdaten an den Mutterkonzern Facebook weitergibt. Das ist datenschutzrechtlich natürlich höchst bedenklich. Googeln Sie mal „WhatsApp und Datenschutz" oder „WhatsApp im Gesundheitswesen".

Doch was sind die Alternativen? Und wie weit sind diese verbreitet?

Signal

Signal ist ein kostenloser Messenger, der seinen Programmcode öffentlich zugänglich macht. Er wirbt damit, dass er sicher ist und die Privatsphäre optimal schützt. Angeblich wurde er sogar von Whistleblower und Datenschutzaktivist Edward Snowden genutzt. Signal wird von einer gemeinnützigen Stiftung mit Sitz im Silicon Valley in Kalifornien betrieben. Die Server stehen ebenfalls in den USA, und genau darin liegt leider das Problem. Damit lässt sich Signal im beruflichen Umfeld nicht DSGVO-konform nutzen. Im privaten Bereich ist Signal jedoch eine hervorragende Alternative zu WhatsApp. Und seit WhatsApp vor Kurzem Änderungen seiner Datenschutzrichtlinie angekündigt hat, haben sich etliche Menschen Signal heruntergeladen und damit auch zu einer höheren Verbreitung dieses Messengers beigetragen.

Threema

Das von einer Schweizer Firma betriebene Threema ist auf Datenschutz und Datenvermeidung ausgelegt und erfordert für die Nutzung weder eine Telefonnummer noch sonstige personenbezogene Angaben. Was seine Verbreitung ausbremst, ist die Tatsache, dass es nicht umsonst ist. Es kostet einmalig knapp vier Euro und kann dann (zumindest theoretisch) lebenslang genutzt werden. Für Firmen hat Threema die Variante Threema Work im Angebot. Obwohl nicht in der EU ansässig (die Schweiz ist der EU nicht beigetreten), hat sich der Messenger die Einhaltung der DSGVO auf die Fahne geschrieben. Dann könnte man ihn doch auch im beruflichen Umfeld ohne Weiteres nutzen, werden Sie jetzt denken. Und die Antwort ist: Jein.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 7. November 2019 ein Whitepaper veröffentlicht, das technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich definiert. Darin wird unter anderem gefordert, dass eine Messenger-App über eine separate Authentifizierung, zum Beispiel per PIN, verfügen muss. Sie muss weiterhin die Möglichkeit haben, Daten auf dem Smartphone verschlüsselt abzulegen. Beides kann Threema, allerdings muss es in den Einstellungen des Messengers extra eingestellt werden. Das wissen jedoch die wenigsten Nutzer. Das Whitepaper ist abrufbar unter
www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf

Die Funktion eines „sicheren Briefumschlages" ist an der SSL-Verschlüsselung erkennbar. Das sieht man auf einen Blick an den fünf Buchstaben „https" und dem Symbol eines kleinen Schlosses.

SPEZIELLE MESSENGER-APPS FÜR DEN GESUNDHEITSBEREICH

Siilo (https://www.siilo.com/de)
Siilo ist ein kostenfreier, sicherer Messenger für medizinische Teams, der nach eigenen Aussagen strikt DSGVO-konform ist und die technischen Datenschutzanforderungen des Whitepapers erfüllt. Betrieben wird er von einer niederländischen Firma in Amsterdam. Die Datenschutzmaßnahmen umfassen unter anderem eine Ende-zu-Ende-Verschlüsselung, eine automatische Löschung von Nachrichten nach 30 Tagen, den Schutz durch PIN-Code/Touch oder Face-ID, die Verifizierung aller Nutzeridentitäten und einiges mehr. Darüber hinaus stellt Siilo zahlreiche Tools bereit, die dabei helfen, Patientendaten zu anonymisieren und zu schützen. Wenn Siilo kostenlos ist, womit verdient die Siilo Holding B.V. denn dann ihr Geld, werden Sie sich womöglich fragen. Siilo bietet für Institutionen wie Krankenhäuser oder Medizinische Fachgesellschaften Lösungen an, die über die reine Messenger-Funktion hinausgehen. Siilo hat Dr. Christine Trutt-Ibing selbst schon auf ihrem Smartphone installiert und getestet. Der Messenger erscheint ihr recht ausgereift zu sein und auf der Website von Siilo finden sich ausführliche Informationen.

Weitere Messenger für das Gesundheitswesen:
- AMP.chat (**https://amp.chat**)
- CONSIL!UM (**https://www.consilium-med.de**)
- WEDOO (**https://wedoo-care.com**)

Der beste medizinische Messenger nützt jedoch nichts, wenn er nicht verbreitet ist!

Tipp: Sprechen Sie sich mit Ärztenetzen, Kliniken vor Ort und anderen Einrichtungen aus dem Gesundheitswesen ab und führen Sie gemeinsam einen Messenger ein. Leider richten sich diese Messenger-Apps wieder nur an Health Professionals. Eine Kommunikation mit Patienten ist nicht vorgesehen.

LÖSUNGEN FÜR DIE SICHERE KOMMUNIKATION MIT PATIENTEN

Wie bereits erwähnt, wird hier die elektronische Patientenakte (ePA) neue Möglichkeiten schaffen.
- **Online-Sprechzimmer (https://www.meinarztdirekt.de)**

Der Allgemeinmediziner Dr. med. Michael Gurr stellt mit seinem Start-up-Unternehmen eine Online-Plattform zur Verfügung, über die sich Arzt und Patient sicher schriftlich austauschen können. Der Arzt kann einen Patienten, der bei ihm bereits in Behandlung ist, in sein Online-Sprechzimmer einladen.

VIDEOKONFERENZEN

Durch die Corona-Krise mussten und müssen noch viele Präsenzveranstaltungen ausfallen. Das betrifft Fortbildungsveranstaltungen genauso wie Fallkonferenzen oder Balint-Gruppen. Als Konsequenz werden diese Treffen nun häufig als Videokonferenz durchgeführt.

Mit Zoom, Microsoft Teams, Cisco Webex Meetings, GoToMeeting und anderen Videokonferenzsystemen haben inzwischen viele Ärzte und Psychotherapeuten im privaten oder beruflichen Umfeld Bekanntschaft gemacht. Doch worauf ist gerade im beruflichen Umfeld zu achten?

Hierzu müssen zunächst verschiedene Anwendungsfälle betrachtet werden.

1. Videokonferenzen im Rahmen von Fortbildungsveranstaltungen (sog. Webinare)
2. Videokonferenzen mit Kollegen (Stichwort: Fallbesprechungen, Balintgruppen)
3. Videokonferenzen mit Kollegen, die mit den Krankenkassen abgerechnet werden können (Fallbesprechungen, Telekonsile)

Je nach Anwendungsfall sind die Anforderungen an den Datenschutz unterschiedlich. Und sicherlich ist jedem klar, dass das Sicherheitsniveau höher sein muss, wenn Patientendaten ins Spiel kommen.

Das Problem bei den anfangs genannten Diensten besteht darin, dass es sich um amerikanische Firmen handelt, die ihre Server in aller Regel in den USA betreiben und die nicht der europäischen Datenschutz-

grundverordnung (DSGVO) unterworfen sind. Bei Fortbildungsveranstaltungen ohne Vorstellung von Kasuistiken stellt das kein allzu großes Problem dar. Bei Fallbesprechungen und dem Austausch von Patientenbefunden (Röntgenbilder, Laborwerte etc.) sieht das jedoch anders aus. Hier ist es relevant, ob Daten ins Nicht-EU-Ausland abfließen können.

Bei Videokonferenzen, die mit den Krankenkassen abgerechnet werden sollen (Fallbesprechungen, Telekonsile), ist die Sache wiederum klar: Hier können nur Systeme zum Einsatz kommen, die von der KBV zertifiziert sind (**www.kbv.de/html/videosprechstunde.php**). Bei den Videosprechstundentools sind je nach Anbieter und Tarif auch Konferenzen mit mehreren, allerdings nicht allzu vielen Teilnehmern möglich.

Doch wie sieht es beim Anwendungsfall 2, den Videokonferenzen im Rahmen von Fallbesprechungen und Balintgruppen, aus? Hier kann auf die amerikanischen Anbieter nur zurückgegriffen werden, wenn Patientendaten ausschließlich anonymisiert kommuniziert und verwendet werden. Und wahrscheinlich runzeln die Datenschützer auch hier die Stirn.

Eine interessante Alternative ist womöglich TeamViewer Meeting. Die Firma TeamViewer ist bisher vor allem für ihre Fernwartungssoftware bekannt, die in vielen Praxen installiert ist, damit IT-Dienstleister bei Problemen schnell helfen können. Das Unternehmen mit Sitz in Deutschland bietet jedoch mit TeamViewer Meeting auch eine Videokonferenz-Lösung an, die nach ISO 9001 zertifiziert und DSGVO-konform ist. TeamViewer Meeting arbeitet mit Ende-zu-Ende-Verschlüsselung, Zwei-Faktor-Authentifizierung und Meeting-Passwörtern. Und für bis zu 5 Teilnehmer ist die Software kostenlos.
https://www.teamviewer.com/de/meeting/

Egal für welche Lösung(en) Sie sich entscheiden, bitte denken Sie daran, mit dem Anbieter des Videokonferenzsystems einen Auftragsverarbeitungsvertrag gemäß DSGVO abzuschließen.

ALLGEMEINE SICHERHEITSHINWEISE FÜR VIDEOKONFERENZEN

- Mikrofon und Kamera am Rechner nur bei Bedarf aktivieren
- Nach der Videokonferenz sollten beide wieder deaktiviert werden (am besten USB-Kabel abziehen)
- Falls das USB-Kabel nicht abgezogen werden kann, Webcam immer abdecken, wenn nicht in Gebrauch

Dr. Christine Trutt-Ibing

Dr. med. Christine Trutt-Ibing

Dr. med. Christine Trutt-Ibing ist Ärztin und Internetexpertin. Mit ihrer Firma CTI Internetlösungen für Ärzte erstellt und betreut sie seit 2009 Praxiswebsites für Ärzte. Sie berät Arztpraxen außerdem zu den Themen digitale Onlinetools.

Dr. Trutt-Ibing ist auch Referentin im Rahmen des Fortbildungsprogramms der KV Hessen. Die Termine für 2021 sind:

- Social Media – Chancen und Risiken neuer Medien am Mittwoch, 10. November 2021, 15.00–18.00 Uhr in der KV in Frankfurt
- Umgang mit Bewertungsportalen am Freitag, 07. Mai 2021, als Onlinefortbildung und Mittwoch, 22. September 2021, in Espenau, jeweils 15.00–18.00 Uhr

Anmelden können Sie sich unter **www.kvhessen.de/fortbildungsprogramm**