Foto: tostphoto – stock.adobe.com

Social Media in der Praxis

Termin-Management per WhatsApp: Was geht, was geht nicht?

Für Datenschützer ist es ein Dauerthema: Die Nutzung von sozialen Netzwerken durch Ärzte und Zahnärzte. Aufgrund der großen Zahl von Nutzern gehört für eine steigende Zahl von Praxen die Präsenz in den sozialen Netzwerken zu einer effektiven Kommunikation dazu, um (neue) Patienten zu erreichen. Ein Fallbeispiel zeigt, worauf es dabei ankommt.

Anders als bei Unternehmen, die soziale Medien schon lange und intensiv nutzen, diskutieren Expertinnen und Experten bereits seit Jahren darüber, in welchem Umfang man im Gesundheitswesen auf Online-Dienste und soziale Netzwerke zurückgreifen könnte und auch dürfe. Vor allem der fachliche Austausch von (Zahn-)Ärzten untereinander ist seit Jahren ein Thema in Fachpublikationen, in denen stets auch auf die ärztliche Schweigepflicht und die Bestimmungen des §203 StGB verwiesen wird.

Welche Fallstricke es in diesem Bereich gibt, lässt sich an einem konkreten Beispiel und einer häufigen Fragestellung aus der Praxis beschreiben: Kann ein soziales Netzwerk genutzt werden, um Termine mit Patienten abzustimmen oder Terminerinnerungen zu versenden?

Foto: Hans Schenkel

Dr. Thomas H. Lenhard ist ein international anerkannter Experte für Informationstechnologie und Datenschutz. Er greift auf seinen umfangreichen Erfahrungsschatz aus drei Jahrzehnten Datenschutz und Datensicherheit zurück und ist u.a. als Datenschutzbeauftragter für die DGI e.V. umfassend tätig.

Der US-amerikanische Anbieter des im deutschen Sprachraum sehr verbreiteten Dienstes WhatsApp stellt eine sogenannte API zur Verfügung. API steht für „Application Programming Interface“ und bezeichnet die Möglichkeit, bestimmte Dienste oder Funktionen in andere Systeme zu integrieren oder daran anzudocken. Die Besonderheit dieser API liegt darin, dass bei deren Nutzung nicht beliebig Daten vom Anbieter des Dienstes erhoben werden können.

Eine umfassende Prüfung des Einzelfalls durch den Datenschutzbeauftragten eines MVZ kam Anfang des Jahres 2023 zu dem Ergebnis, dass die API unter bestimmten Voraussetzungen datenschutzkonform eingesetzt werden könnte, um den Patienten Terminerinnerungen zu senden. Einige der grundlegenden Voraussetzungen für die Zulässigkeit der Nutzung dieses Dienstes waren dabei:

- das Vorliegen einer aktiven Zustimmung des Patienten zur Nutzung dieses Kommunikationsweges,
- die umfassende Information des Patienten über Art, Umfang, Verwendung und Speicherung der über ihn erhobenen Daten sowie über seine Rechte als Betroffener einer Datenverarbeitung
- und insbesondere auch die Gewährleistung, dass der betroffene Patient jederzeit erfolgreich der weiteren Nutzung seiner Daten zur Kommunikation auf der entsprechenden Plattform widersprechen kann.

Ein betroffener Patient muss jederzeit erfolgreich der weiteren Nutzung seiner Daten zur Kommunikation auf einer Plattform widersprechen können.

Die Einbindung wäre demnach so möglich gewesen, dass im Patientenmanagement ein Häkchen die Zustimmung zur Nutzung der Plattform repräsentiert hätte, das von der Praxis nach einer schriftlichen Zustimmung gesetzt worden wäre. Zusätzlich wäre es noch erforderlich gewesen, die Kommunikationsdaten des Patienten zu erfassen, über die er mittels des entsprechenden Dienstes erreichbar ist. Die schriftliche Zustimmung muss nachvollziehbar dokumentiert und wiederauffindbar archiviert sein.

Bezüglich des Einsatzes des entsprechenden Dienstes bestanden, vorbehaltlich der einzuhaltenden Rahmenbedingungen, seitens des zuständigen Datenschutzbeauftragten keine Bedenken. Nach eingehender Prüfung ist der Datenschützer zu dem Schluss gelangt, dass „eine datenschutzkonforme Nutzung der entsprechenden Plattform zum Versenden von Terminerinnerungen – nach aktiver und dokumentierter Zustimmung des Patienten – grundsätzlich möglich sei“.

Dennoch wurde das Projekt letztendlich nicht umgesetzt – aus guten Gründen. Zunächst verweigerte ein namhafter Hersteller eines Patientenmanagementsystems die Integration der API in das System des MVZ. Damit war die einfachste und effizienteste Vorgehensweise, das Vorhaben zu realisieren, nicht umsetzbar. Eine Begründung für die ablehnende Haltung des Softwareunternehmens ist bislang nicht bekannt.

Schließlich bot ein weiteres Dienstleistungsunternehmen an, auf die Datenbank des Patientenmanagementsystems zuzugreifen und somit die gewünschte Funktionalität doch noch dem MVZ zur Verfügung zu stellen. Der Datenschutzbeauftragte des MVZ wurde diesbezüglich erneut konsultiert und prüfte die angebotene Lösung auf deren Konformität hinsichtlich datenschutzrechtlicher Bestimmungen. Dabei kam es zu folgenden Feststellungen:

- Der Abzug von Daten aus der Datenbank konnte nicht auf Patienten beschränkt werden, die der Nutzung des sozialen Netzwerkes zuvor zugestimmt hatten.
- Die extrahierten Patientendaten sollten nicht in einer Datenbank innerhalb des MVZ, sondern vollständig in einer Cloud eines US-amerikanischen Anbieters gespeichert werden.
- Informationen über eine Sondergenehmigung der Nutzung dieser US-Cloud durch eine Bundesbehörde, die vom Anbieter zur Verfügung gestellt wurden, standen nicht im Zusammenhang mit der geplanten Lösung und waren daher nicht relevant. Eine Rückfrage bei der entsprechenden Behörde untermauerte die Zweifel an der Zulässigkeit der angebotenen Lösung.

Zum Zeitpunkt dieser Prüfung galten die USA – was die Verarbeitung personenbezogener Daten angeht – noch als unsicheres Drittland. Die Prüfung des Falles führte daher zu größten Bedenken: Ein ausreichendes Niveau des Datenschutzes konnte nicht bestätigt werden. Ein wesentlicher Grund für diese Vermutung war die Zweckänderung der Nutzung von Patientendaten, die – aller Voraussicht nach – ohne Zustimmung der Betroffenen in ein unsicheres Drittland übertragen werden sollten.

Das Problem im konkreten Projekt war demnach nicht die Nutzung des sozialen Netzwerks, sondern die geplante technische Umsetzung des Vorhabens.

Veränderte Rechtslage. Am 10. Juli 2023 wurde ein Angemessenheitsbeschluss der EU-Kommission hinsichtlich des Datenaustauschs mit den USA verabschiedet. Grundsätzlich bedeutet dies, dass für eine Datenverarbeitung in den USA das gleiche Datenschutzniveau angenommen werden kann wie für Verarbeitungen innerhalb der EU. Natürlich werden sich Anbieter nunmehr auf diesen Beschluss berufen, um ihre Produkte und Dienste verkaufen zu können.

Diesem Beschluss war jedoch am 11. Mai 2023 eine Entschließung des EU-Parlaments vorausgegangen, in dem sich das Parlament vehement gegen den geplanten Beschluss der EU-Kommission aussprach. Die Kommission hatte sich daher über massive Bedenken und Entschließungen hinweggesetzt, die Fachexperten, der europäische Datenschutzausschuss und das EU-Parlament formuliert hatten.

Nach veränderter Rechtslage kann grundsätzlich für eine Datenverarbeitung in den USA das gleiche Datenschutzniveau angenommen werden wie in der EU.

Klagen vor dem EuGH werden folgen. NOYB, die Organisation um den österreichischen Juristen und Datenschützer Max Schrems, der bereits zwei Abkommen der EU mit den USA vor dem Europäischen Gerichtshof zu Fall gebracht hat, hat bereits eine weitere Klage vor dem EuGH in Aussicht gestellt. Dies bedeutet, dass die EU-Kommission eine Situation der Rechtsunsicherheit geschaffen hat.

SICHERES VORGEHEN BEI UNSICHERER RECHTSLAGE

1. Lassen Sie jede neue Software oder jeden neuen Dienst (insbesondere webbasierte Dienste), die Sie in Ihrer Praxis einsetzen wollen, von Ihrem Datenschutzbeauftragten oder einem Datenschutzexperten eingehend prüfen, bevor Sie einen Vertrag unterzeichnen. Lassen Sie sich das Prüfergebnis für Ihre Unterlagen in schriftlicher Form geben.

2. Beachten Sie das Postkartenprinzip, das bereits im Bereich der E-Mail eingesetzt wird: In ein soziales Netzwerk sollten Sie keine Informationen einstellen, die Sie nicht auch bedenkenlos auf der Rückseite einer Postkarte versenden könnten.

3. Seien Sie kritisch hinsichtlich der Aussagen von Vertriebsmitarbeitern von Anbietern webbasierter Dienste. Lassen Sie sich gegebenenfalls schriftlich bestätigen, dass die Daten ausschließlich in Ihrer Organisation oder bei einem unzweifelhaft vertrauenswürdigen Anbieter gespeichert werden.

4. Beachten Sie, dass betroffene Patienten über jede Zweckänderung – soweit diese überhaupt zulässig ist – informiert werden müssen.

5. Dokumentieren Sie die Zustimmungen der Patienten, soweit Sie mit diesen über soziale Netzwerke kommunizieren möchten.

6. Soweit Daten außerhalb Ihrer Praxis gespeichert werden, liegt in aller Regel eine Auftragsverarbeitung nach Art. 28 DSGVO vor. Die entsprechenden Voraussetzungen für eine Zulässigkeit der Auftragsverarbeitung sind vor Vertragsabschluss zu klären.

7. Überlegen Sie, welche Folgen es für Ihre Praxis haben könnte, wenn der Angemessenheitsbeschluss der EU-Kommission hinsichtlich der USA vom EuGH gekippt wird.

Unsichere Rechtslage. Über allen Institutionen – Unternehmen oder Praxen –, die aufgrund des Beschlusses der EU-Kommission nunmehr personenbezogene Daten in die USA oder in Systeme von US-Unternehmen übermitteln, wird ein drohender Prozess beim EuGH wie ein Damoklesschwert schweben. Sollte der EuGH den Angemessenheitsbeschluss kippen, dürfte es in aller Regel keine triviale Aufgabe sein, Systeme zu wechseln und die Daten wieder aus den USA in die EU zurückzuholen.

Fazit: Die Nutzung sozialer Netzwerke für ausgewählte unkritische Zwecke, wie eine Terminerinnerung durch Zahnarztpraxen ist grundsätzlich möglich. Dabei ist jedoch eine Vielzahl von Voraussetzungen zu erfüllen. Es wäre sicherlich wünschenswert, dass die gängigen Anbieter von Patientenverwaltungssystemen hier eine Integrationsmöglichkeit anbieten, bei der sich der Zahnarzt darauf verlassen kann, dass es sich um ein standardisiertes Verfahren handelt, das bereits auf seine datenschutzrechtliche Zulässigkeit geprüft wurde.

Es ist sicherlich einfacher, ein Standardverfahren beim Anbieter zu prüfen, als die konkrete Umsetzung in jeder Zahnarztpraxis prüfen zu müssen. Hier sind die Anbieter von Systemen gefordert, zeitgemäße und datenschutzkonforme Lösungen anzubieten und so der Nachfrage durch die Praxen (Kunden) Rechnung zu tragen.

Hier geht es zur Stellungnahme NOYB zum Angemessenheitsbeschluss der EU-Kommission:
https://noyb.eu/de/european-commission-gives-eu-us-data-transfers-third-round-cjeu

Hier finden Sie die Entschließung des EU-Parlaments hinsichtlich des Angemessenheitsbeschlusses für die USA:
https://www.europarl.europa.eu/doceo/document/TA-9–2023–0204_DE.html

→ **Dr. Thomas H. Lenhard**