Informationen zum Datenschutz – Patienten-App

Stand: 10.11.2023

Herzlich willkommen!

Nachfolgend informieren wir Sie über den Umgang mit Ihren personenbezogenen Daten bei der Nutzung unserer Anwendung und Ihre diesbezüglichen Rechte. Wir überarbeiten diese Informationen bei Bedarf und halten Sie online unter www.thieme-compliance.de/datenschutz/patienten-app/ jederzeit auf dem neuesten Stand. Zugunsten der Lesbarkeit verzichten wir nachfolgend auf Gender-Formulierungen.

Wichtig: Für medizinische Fragen ist ausschließlich Ihr Behandler zuständig. Dasselbe gilt, wenn Sie die E-Mail (Link zur Patientenanwendung) oder SMS (Token) nicht erhalten haben (auch nicht im Spam-Ordner). Bitte nehmen Sie deshalb auch die Datenschutzinformationen Ihres Behandlers zur Kenntnis.

Inhaltsverzeichnis

1. Verantwortlichkeiten

Verantwortlich für die Verarbeitung Ihrer personenbezogenen und medizinischen Daten ist Ihr Behandler (von Ihnen gewählte Praxis, Klinik, andere medizinische Einrichtung).

Als Nutzer der Anwendung tragen Sie die Mitverantwortung, dass kein Unbefugter Zugriff auf das von Ihnen genutzte Gerät bzw. die Daten erhalten kann.

2. Zweck, Art, Rechtsgrundlage und Umfang der Datenverarbeitung

Wofür werden Ihre Daten benötigt und auf welcher Rechtsgrundlage verarbeiten wir diese.

a) Zweck der Datenverarbeitung
Die Anwendung ermöglicht es dem Behandler, Ihnen als Patient wichtige Informationen (zu Behandlung/Aufenthalt usw.) zeitgemäß elektronisch sowie orts- und systemunabhängig zur Verfügung zu stellen. So können relevante Daten frühzeitig erfasst und in den Behandlungsprozess eingesteuert werden, um unnötigen Stress für alle Beteiligten zu vermeiden.

Die Nutzung der Patienten-App ist immer freiwillig und kostenlos für Sie. Nach Übermittlung der Daten auf Ihrem Endgerät an den Behandler werden Ihre bisher erfassten Daten sofort gelöscht. Unvollständige Daten, die Sie nicht an den Behandler übermitteln, werden nach spätestens 14 Tagen automatisch gelöscht.

b) Art und Umfang der Datenverarbeitung

Die Patienten-Anwendung ist eine sogenannte Progressive Web App. Diese rufen Sie als Patient direkt über den per E-Mail vom Behandler zugesandten persönlichen Link auf, ein App-Store ist nicht erforderlich. Die App liegt in der besonders sicheren Microsoft Azure Public Cloud („Azure“) in einem gesondert abgeschirmten Bereich und kann auf jedem von Ihnen gewählten internetfähigen Endgerät im Internetbrowser geöffnet werden.

Zum Schutz Ihrer Privatsphäre kann die Patienten-App nur benutzt werden, wenn Sie sich mit dem per E-Mail an Sie persönlich übertragenen individuellen Link und zusätzlich über den per SMS auf Ihr Mobiltelefon übertragenen Token (PIN) anmelden. Erst dann können Sie alle für Sie wichtigen Informationen und Daten abrufen und die Fragen bearbeiten. In der Azure Cloud wird dazu für Sie ein zeitlich begrenzter Account angelegt. Der Account enthält weder Ihren Namen noch Ihre E-Mail-Adresse, sondern nur eine eindeutig zuordenbare Identifikationsnummer („UUID“) als Pseudonym.

Auf dem von Ihnen gewählten privaten Endgerät werden Ihre Antworten nur im Arbeitsspeicher vorgehalten, solange Sie daran arbeiten. Eine lokale Speicherung auf dem Gerät findet zu Ihrer Sicherheit nicht statt. Die App überträgt in regelmäßigen Abständen einen verschlüsselten Zwischenstand Ihrer Antworten, damit Ihre bisherigen Antworten nicht verloren gehen. Melden Sie sich ab, wird ebenfalls ein Zwischenstand übertragen.

Zum Schutz Ihrer Privatsphäre auch unterwegs und zuhause meldet die Patienten-App Sie ab, wenn Sie in dieser Anwendung länger als 10 Minuten nicht aktiv sind (Fragen beantworten oder Videos ansehen). Sie können sich dann einfach mit Ihren Zugangsdaten wieder anmelden (Link, Token).

Zur Übertragung werden Ihre Daten je nach Informationsart (Fragen, Antworten, Identifikationsdaten) auf Basis Ihrer UUID in getrennten Datenbanken auf Azure verschlüsselt gespeichert und von dort automatisch an Ihren Behandler übertragen und in sein Patientenverwaltungssystem integriert.

Die komplette Datenverarbeitung in der Azure Cloud erfolgt also nicht nur pseudonymisiert, sondern auch mit Hilfe getrennter Speicherplätze. Zusätzlich werden alle Daten nach aktuell sicherem Standard verschlüsselt. Zugriff erhalten nur Sie als Patient selbst (über die Patienten-App) – und Ihr Behandler, sobald Sie Ihren vollständig bearbeiteten Datensatz in der App an die medizinische Einrichtung gesendet haben. Auch dieser erhält Ihre Daten verschlüsselt und entschlüsselt sie nach Erhalt zur Vorbereitung auf das persönliche Aufklärungsgespräch mit Ihnen.

Übertragen Sie Ihren Datensatz nicht an den Behandler, werden die Daten automatisch nach einem festgelegten Zeitraum (z.B. nach 14 Tagen) gelöscht, soweit dies technisch möglich ist (je nach Berechtigungen auf dem Gerät). Achten Sie deshalb darauf, dass Sie die Fragen möglichst zügig beantworten und an Ihren Behandler senden.

Sobald Ihre Daten vollständig erfolgreich an Ihren Behandler übertragen sind, werden sie automatisch aus der Azure Cloud gelöscht. Die Weiterverarbeitung (Vervollständigung im Arztgespräch) der Daten erfolgt ausschließlich innerhalb der Infrastruktur Ihres Behandlers. Hier werden Ihre Anamnesedaten zusammengeführt, gespeichert und als PDF archiviert.

Protokollierungen und Auswertungen finden bei der Patienten-App, beim Behandler und auf Azure systemseitig im Hintergrund automatisiert statt. Diese Informationen benötigen Behandler und Hersteller zur Sicherstellung des ordnungsgemäßen Betriebs, zur Verbesserung der Benutzerfreundlichkeit, zur Systemoptimierung, zur Abwehr von Angriffen und zu Nachweiszwecken. Ein direkter Personenbezug ist nicht relevant. Auch wenn beispielsweise die IP-Adresse der genutzten Verbindung standardmäßig in solchen Logfiles enthalten ist, wird ein möglicher Rückschluss auf einen Betroffenen nicht hergestellt. Azure erhält

zudem ausschließlich pseudonymisierte verschlüsselte Daten.

c) Rechtsgrundlage aus Sicht als Hersteller der Anwendung

Personenbezogene Daten erheben, speichern und nutzen wir nur im zulässigen Rahmen. Als Hersteller der Anwendung verfolgen wir das Datenschutz-Prinzip der Datenminimierung und vermeiden die Verarbeitung personenbezogener Daten soweit möglich. Daher ist die Thieme Compliance GmbH kein Auftragsverarbeiter im klassischen Sinn. Dennoch verpflichten wir uns in einer Vereinbarung zur Auftragsverarbeitung zur Einhaltung der vielfältigen Datenschutzanforderung.

- Erfüllung des Vertrags-/vertragsähnlichen Vertrauensverhältnisses (Art. 6 Abs. 1 lit. B DSGVO)
  z.B. zur Authentifizierung befugter Nutzer, zur Bereitstellung zugeordneter Informationen sowie zur Lizenzverwaltung (nur gegenüber dem Behandler);

  Wir als Hersteller erhalten und verarbeiten keine Patientendaten, da wir diese nicht benötigen. Schickt der Behandler uns unaufgefordert solche Daten, werden diese von uns datenschutzkonform gelöscht und der Absender darauf hingewiesen, dies nicht zu tun.

- Datenverarbeitung im Auftrag (Art. 28 DSGVO)
  Im Einzelfall kann eine vertiefte Fehleranalyse durch ein externes Entwicklerteam erforderlich werden, bei der im Bedarfsfall auch Patientendaten betroffen sein können. Eine solche Analyse erfolgt ausschließlich auf Basis einer Datenverarbeitung im Auftrag des Behandlers und mit besonderen Schutzmaßnahmen für die Datenübermittlung und Verarbeitung. Details siehe nächstes Kapitel.

- Verfolgung berechtigter Interessen unseres Unternehmens (Art. 6 Abs. 1 lit. F DSGVO)
  z.B. zur Sicherstellung des ordnungsgemäßen Funktionierens der Anwendungen und Funktionen auf unterschiedlichen Endgeräten, zur Sicherheit personenbezogener Daten innerhalb der Anwendung sowie auf dem Übertragungsweg und zur Optimierung der Bedienbarkeit (Usability), sofern nicht schwerwiegende Interessen der Betroffenen überwiegen.

3. Datenempfänger

Nachfolgende Empfänger können Daten durch Nutzung der App erhalten bzw. weiterverarbeiten. Denken Sie daran, dass Sie selbst darauf Einfluss haben und nehmen Sie Ihre Verantwortung für Ihre besonders schützenswerten Daten gewissenhaft wahr.

a) Die behandelnde Stelle als Verantwortlicher (Arztpraxis, Klinik, andere medizinische Einrichtung)

Ihr Behandler erhält von Ihnen die für die vertraglich vereinbarte Behandlung erforderlichen Daten über die Patienten-Anwendung direkt von Ihnen. Die Daten werden über die Azure Cloud-Schnittstelle verschlüsselt an ihn übertragen und erst in seiner Infrastruktur zur weiteren Verarbeitung entschlüsselt.

b) Der Betroffene (Patient)

Als Patient erhalten Sie eine E-Mail mit dem Link zum Download und der Nutzung der Patienten-Anwendung. Per SMS wird zusätzlich ein Zugangscode gesendet. Beide Bestandteile werden zur sogenannten 2-Faktoren-Authentifizierung zusammen benötigt, ohne die sich die App nicht verwenden lässt. Verwahren Sie diese daher vertraulich.

c) Der Eigentümer/Besitzer des vom Patienten gewählten Endgeräts

Achten Sie darauf, möglichst ein eigenes Endgerät zu verwenden, auf dem Sie den Zugriff steuern können. Sonst erhalten durch Sie möglicherweise unerwünschte Dritten (Haushaltsangehörige, Internetcafé-Betreiber usw.) Zugriff auf Ihre Krankengeschichte.

d) Thieme Compliance GmbH (Hersteller der App, Bereitsteller der Filme in der App)

Nur der Behandler kann unseren Support bei technischen Problemen in Anspruch nehmen. Die Patienten-Anwendung ist davon nicht betroffen.

e) Weitere Partner zur Vertragserfüllung (Outsourcing, Auftragsverarbeitung)

Die Zusendung des Links zur Patienten-Anwendung erfolgt derzeit ausschließlich über den E-Mail-Server Ihres Behandlers.

Der Token wird per SMS vom sorgfältig ausgewählten deutschen Dienstleister seven.io an die Ihnen als Patient angegebene Mobilrufnummer übertragen.

Bei besonderen technischen Problemen beim Behandler setzen wir unsere Entwicklungsspezialisten ein. Im Einzelfall können komplette Datensätze benötigt werden, um einen Fehler einzugrenzen und eine Lösung erarbeiten zu können. Die Datenübertragung erfolgt im konkreten Bedarfsfall, soweit wir als Hersteller dies steuern können, ausschließlich über eine auf hochsensible Daten spezialisierte Datentransfer-Plattform in Deutschland. Die Verarbeitung der gesamten Daten erfolgt ausschließlich zur Fehleranalyse und daher für einen sehr begrenzten Zeitraum.

Da die pseudonymisierten Daten zusätzlich verschlüsselt sind, findet eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR), soweit nachfolgend nicht ausdrücklich anders beschrieben, nicht statt und ist auch nicht geplant. Mit Microsoft Deutschland GmbH ist vereinbart, nur Serverstandorte in der EU einzusetzen; ab Herbst 2022 soll dies laut Microsoft für alle ihre Server Standard werden. Darüber hinaus werden alle Daten nur pseudonym und zusätzlich wirksam verschlüsselt an Azure übertragen. Durch eine strikte Trennung der Funktionalitäten ist außerdem immer nur eine Teilmenge der Daten verfügbar.

Wir geben Ihre Daten nicht an unbefugte Dritte weiter und verkaufen diese selbstverständlich nicht.

4. Wahrung Ihrer Rechte als „Betroffener“ im Sinne des Datenschutzrechts

a) Produktdatenschutz

Gemäß den Anforderungen der DSGVO hinsichtlich der Produkte und Dienstleistungen, die wir auf dem europäischen (deutschen) Markt anbieten, bieten wir vielfältige Ansätze zur entsprechenden datenschutzkonformen Technikgestaltung und datenschutzfreundliche Voreinstellungen, soweit uns dies – etwa im Hinblick auf die Einbindung in der Infrastruktur des Behandlers – möglich ist.

Für die Wirksamkeit und Nachhaltigkeit der getroffenen Datenschutzmaßnahmen stehen neben der Geschäftsleitung (als den Verantwortlichen) und dem Datenschutz auch die Compliance (standardisiertes Vorgehen zur kontinuierlichen Optimierung unseres Datenschutzniveaus) sowie bewährte externe Datenschutz-Spezialisten zur Verfügung.

b) Kontaktaufnahme mit uns als Hersteller der Anwendung

Bei Kontaktaufnahme mit uns, etwa per E-Mail oder Telefon, speichern und nutzen wir Ihre Angaben zur Bearbeitung Ihrer Anfrage und im Rahmen unserer Aufbewahrungs- und Nachweispflichten. Sofern Ihre Anfrage auch den Behandler betrifft, sind wir verpflichtet, diese bei konkretem Handlungsbedarf auch an den Verantwortlichen weiterzuleiten, damit dieser seinen Pflichten ebenfalls nachkommen kann.

c) Maßnahmen aus Herstellersicht zur Wahrung Ihrer Rechte als Betroffener

- Recht auf Information/Transparenz (Art. 13, 14 DSGVO):
  Erhalten Sie von unserer Seite mit diesem Dokument

- Recht auf Auskunft (Art. 15 DSGVO):
  Wir unterstützen den Behandler im Rahmen unserer (begrenzten) Möglichkeiten bei Anfragen

- Recht auf Berichtigung (Art. 16 DSGVO):
  Obliegt dem Behandler, da wir keinen Zugriff auf Ihre Daten haben

- Recht auf Löschung (Art. 17 Abs. 1 DSGVO):
  Systemseitig umgesetzt, soweit möglich; die weitere Datenlöschung obliegt dem Behandler

- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO):
  Obliegt dem Behandler

- Recht auf Datenübertragbarkeit (Art. 20 DSGVO):
  Der Behandler kann die von Ihnen eingegebenen Daten im gängigen JSON-Format exportieren und Ihnen auf Wunsch zur Verfügung stellen

- Recht auf Widerspruch (Art. 21 DSGVO):
  Sie können die Nutzung der mobilen Datenerfassung jederzeit abbrechen und die Fragen wie bisher üblich im persönlichen Aufklärungsgespräch beim Behandler beantworten

5. Kontakt für weiterführende Fragen zur App

Für die Verarbeitung Ihrer Patientendaten ist Ihr Behandler und dessen Datenschutzbeauftragter zuständig. Thieme Compliance ist nur für die technischen Daten der App selbst zuständig und kann Ihnen nur hierzu Auskunft erteilen.

a) Hersteller und Betreiber der App

Thieme Compliance GmbH, Am Weichselgarten 30a, 91058 Erlangen
Telefon: +49 9131 93406-40, E-Mail: service@thieme-compliance.de

b) Die zuständige Datenschutzbeauftragte

Unsere ausführlichen Datenschutzinformationen und die aktuellste Fassung dieses Dokuments finden Sie unter www.thieme-compliance.de/datenschutz.

Für Ihre weiteren Datenschutz-Anliegen **hinsichtlich der App** steht Ihnen unser Data Privacy Officer (DPO) gern zur Verfügung, am bequemsten per E-Mail unter datenschutz@thieme-compliance.de.

c) Die zuständige Aufsichtsbehörde

Ihr Beschwerderecht **hinsichtlich einer nicht datenschutzkonformen Datenverarbeitung durch Ihren Behandler (medizinische Einrichtung)** können Sie bei jeder Aufsichtsbehörde ausüben.

6. Datenschutzinformationen der verbundenen Partner

Microsoft Azure:

- Allgemeine Informationen: https://azure.microsoft.com/de-de/overview/trusted-cloud/privacy/
- Durchführung DSFA: https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-dpia-azure
- Adresse: Walter-Gropius-Straße 5 80807 München

Adesso SE (Entwicklung & Test):

- Allgemeine Informationen: https://www.adesso.de/de/
- Informationen zum Datenschutz: https://www.adesso.de/de/datenschutz/datenschutz-neu.jsp
- Adresse: Adessoplatz 1, 44269 Dortmund

EcpliseSource Group (Entwicklung & Test):

- Allgemeine Informationen: https://eclipsesource.com/de/
- Informationen zum Datenschutz: https://eclipsesource.com/de/datenschutz/
- Adresse: Lammstr. 21, 76133 Karlsruhe

seven.io:

- Allgemeine Informationen: https://www.seven.io/de/produkte/sms-versand/
- Informationen zum Datenschutz: https://www.seven.io/de/unternehmen/datenschutz/
- Adresse: Willestr. 4-6, 24103 Kiel