Informationen zum Datenschutz – Patienten-App

Stand: 27.10.2021

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.

Wichtig: Für medizinische Fragen ist ausschließlich der 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 auch die Datenschutzinformationen Ihres Behandlers zur Kenntnis.

Inhaltsverzeichnis

1. Verantwortlichkeiten

Verantwortlich für die Verarbeitung Ihrer personenbezogenen und medizinischen Daten ist der Behandler (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 „Dürfen die das“?

a) Zweck der Datenverarbeitung

Die Anwendung ermöglicht es dem Behandler Ihnen als Patient wichtige Informationen (zur Behandlung/Aufenthalt usw.) zeitgemäß elektronisch sowie orts- und systemunabhängig zur Verfügung zu stellen sowie frühzeitig relevante Daten zu erheben und diese in den Behandlungsprozess einzusteuern, um diesen und weitere relevante Prozesse anzustoßen. Die Nutzung der Patienten-App ist freiwillig. 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 maximal 14 Tagen gelöscht.

b) Art der Datenverarbeitung

Die Patienten-Anwendung ist eine sogenannte Progressive Web App. Diese wird unabhängig von einem App-Store direkt über den zugesandten persönlichen Link auf der besonders sicheren Microsoft Azure Public Cloud („Azure“) auf dem von Patienten gewählten privaten Endgerät im Browser geöffnet. Es besteht zudem die Möglichkeit die Anwendung auf dem Gerät zu installieren.

Die Patienten-App kann nur benutzt werden, wenn sich der Patient mit dem per E-Mail an ihn persönlich übertragenen individuellen Link und zusätzlich über den per Medienbruch übertragenen Token (PIN) authentifizieren kann.

Auf der Azure Cloud wird für den Patienten ein zeitlich begrenzter Account unter einer eindeutig zuordenbaren Identifikationsnummer („UUID“) als Pseudonym angelegt. Dieser sorgt dafür, dass nur der berechtigte Patient sich bei der App anmelden und die für ihn relevanten Informationen/Daten sehen und bearbeiten kann.

Die komplette Datenverarbeitung in der Azure Cloud erfolgt auf Basis der UUID pseudonym und lässt keinen Rückschluss auf die Person zu. Für noch mehr Sicherheit werden alle Daten außer der UUID zusätzlich nach aktuell sicherem Standard wirksam verschlüsselt. Zugriff erhält nur der Patient selbst über die Patientenanwendung und der Behandler nach Übermittlung des Datensatzes an die medizinische Einrichtung.

Ihre Antworten werden auf dem von Ihnen gewählten privaten Endgerät in einem gesonderten Ordner gespeichert, bis Sie diese erfolgreich an Ihren Behandler übertragen.

Erfolgt keine Übertragung werden die Daten nach spätestens 14 Tagen gelöscht, soweit dies technisch über die App möglich ist (je nach Berechtigungen auf dem Gerät). Achten Sie deshalb bitte darauf, dass Sie das Endgerät sorgfältig wählen. In einem Internetcafé können Ihnen nicht nur unbefugte Menschen über die Schulter sehen, sondern Sie haben in der Regel auch keine Kontrolle, ob Ihre Eingaben nicht im Hintergrund ausspioniert werden oder ob diese im Nachhinein tatsächlich gelöscht werden können.

Ihre Daten werden je nach Informationsart auf Basis Ihrer UUID in getrennten Datenbanken auf Azure verschlüsselt gespeichert. Sobald sie vollständig erfolgreich an Ihren Behandler übertragen worden sind (in der Regel täglich, abhängig von der Konfiguration Ihres Behandlers), werden sie von Azure automatisiert gelöscht.

Die Weiterverarbeitung (Überprüfung und Vervollständigung im Arztgespräch) der Daten erfolgt ausschließlich innerhalb der Infrastruktur Ihres Behandlers. Dazu werden Sie in der Anamnesehistorie zum Patienten gespeichert. Zusätzlich werden die Daten 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 ausschließlich pseudonymisierte verschlüsselte Daten.

Die Nutzung der App ist kostenlos und freiwillig.

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.

- 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 Behandler);

  Wir als Hersteller erhalten und verarbeiten keine Patientendaten, da wir diese nicht benötigen. Schickt der Behandler uns unaufgefordert solche Daten, werden sie von uns datenschutzkonform gelöscht und der Behandler 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 Kapitel 4e.

- 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 die 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 benötigt, ohne die sich die App nicht verwenden lässt.

c) Der Eigentümer/Besitzer des vom Patienten gewählten Endgeräts

Achten Sie bitte darauf, möglichst ein eigenes Endgerät zu verwenden, auf dem Sie den Zugriff steuern und vor allem einschränken und Ihre Daten wieder löschen können. Sonst ermöglichen Sie möglicherweise unerwünscht Dritten (Haushaltsangehörige, Internetcafé-Betreiber usw.) den 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)

Für die Zusendung des Links zur Patienten-Anwendung wird entweder der E-Mail-Server vom Behandler oder ein deutscher E-Mail-Provider eingesetzt.

Der Token wird per SMS vom sorgfältig ausgewählten deutschen Dienstleister SMS77 an die vom Patienten angegebene Mobilrufnummer übertragen.

Bei besonderen technischen Problemen beim Behandler setzen wir unsere Entwicklungsspezialisten ein. Im Einzelfall können die hierbei verarbeiteten personenbezogenen oder Gesundheitsdaten zwingend benötigt werden, um den Fehler eingrenzen und eine Lösung erarbeiten zu können.

Die Datenübertragung erfolgt nur im Bedarfsfall, für einen begrenzten Zeitraum und über eine auf hochsensible Daten spezialisierte Datentransfer-Plattform in Deutschland.

Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) findet, soweit nachfolgend nicht ausdrücklich anders beschrieben, nicht statt und ist auch nicht geplant. Bei Microsoft Azure nutzen wir Server in der EU, 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.

f) Dienste auf Ihrem Endgerät

In der Regel bietet Ihnen die Anbieter Ihres Endgerätes oder Ihr Telekommunikationsanbieter die Möglichkeit eines Backups in dessen Cloud, wenn diese Option auf Ihrem Endgerät aktiviert ist. Elemente des Betriebssystems bzw. andere installierte Apps erheben normalerweise im Hintergrund ebenfalls Daten über Sie, Ihren Standort, genutzte Apps, Suchbegriffe oder sogar Nutzungs- und Kommunikationsdaten. Dies gilt vor allem für Dienste mit künstlicher Intelligenz wie etwa Sprachassistenten (Siri, Alexa etc.). Bitte prüfen Sie hierzu die Anbieterinformationen und überprüfen Sie regelmäßig die Datenschutzeinstellungen auf Ihrem Endgerät.

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 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 xml-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 das herkömmliche Aufklärungsgespräch inkl. der Erhebung Ihrer Daten beim Behandler nutzen

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) Frau Blossey 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: Microsoft Ireland Operations, Ltd., Attn: Data Privacy, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland

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

sms77:

- Allgemeine Informationen: https://www.sms77.io/de/
- Informationen zum Datenschutz: https://www.sms77.io/de/unternehmen/datenschutz/
- Adresse: Willestr. 4-6, 24103 Kiel