Stellungnahme EU Datenschutz-Grundverordnung

Thieme Compliance GmbH

11.07.2018

Thieme Compliance GmbH
Am Weichselgarten 30a • 91058 Erlangen
www.thieme-compliance.de

Thieme Compliance

Stellungnahme EU Datenschutz-Grundverordnung

Die EU Datenschutz-Grundverordnung (DSGVO/GDPR) ist seit ihrem Inkrafttreten am 25.05.2016 im Gespräch und uns erreicht verschiedentlich die Frage: „Sind Sie gerüstet für die DSGVO?“ Deshalb wollen wir Sie an dieser Stelle gerne dazu informieren.

Die Thieme Compliance GmbH steht seit 2007 für medizinisch und juristisch fundierte prozessorientierte Patientenaufklärung bei medizinischen Eingriffen. Qualität spielt in diesem Bereich eine besonders große Rolle. Daher ist die Einhaltung gesetzlicher Vorgaben für uns eine Grundanforderung. Dies gilt selbstverständlich auch für die Aspekte des Datenschutzes. Vor mehr als zehn Jahren haben wir unsere Datenschutzorganisation neu strukturiert und passen diese seither systematisch an die wachsenden Anforderungen und Entwicklungen in Datenschutz und Datensicherheit an.

So erfüllen wir viele Anforderungen, die erst jetzt durch die EU-Gesetzgebung zu Pflichtaufgaben geworden sind, beispielsweise die Dokumentation unserer Datenschutztätigkeiten oder auch die Risikoabschätzung von Verfahren mit personenbezogenen Daten.

Die aktuellen Datenschutzanforderungen finden auch in der Design- und Entwicklungsphase unserer Produkte vollumfängliche Berücksichtigung. Eine der neuen Kernanforderung nach DSGVO sind „privacy by design“ und „privacy by default“. Datenschutz wird bereits bei der technischen Produktgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt.

Generell werden bei unseren Produkten keine personenbezogenen Daten, vor allem keine Patientendaten, an Thieme Compliance übermittelt. Vielmehr werden die Produkte in die bestehende Systemlandschaft Ihrer Organisation integriert, entweder über die Nutzung unseres Online-Portals E-Consent oder über die lokal begrenzte Anwendung E-ConsentPro Classic. Auch unsere gedruckten Aufklärungsbögen enthalten bei der Auslieferung keine Daten von Patienten.

E-ConsentPro Classic

Die meisten Aufklärungsbögen von Thieme Compliance enthalten Anamnesefragen an den Patienten. Allerdings handelt es sich sowohl bei gedruckten als auch bei den in der Software E-ConsentPro digital zur Verfügung gestellten Aufklärungsbögen um „leere“, nicht individualisierte Inhalte, die keine Patientendaten enthalten. Diese Daten werden erst in der Klinik oder Praxis eingefügt. Damit werden im Sinne der DSGVO in den Produkten von Thieme Compliance keine Daten gespeichert oder weiterverarbeitet. Es obliegt allein der jeweiligen Institution, die geltenden Datenschutzbestimmungen einzuhalten und beispielsweise von den Betroffenen bei Bedarf entsprechende Einwilligungen einzuholen.

E-ConsentPro mobile

Nach einer Zuweisung aus dem E-ConsentPro (ECP) WebClient heraus wird ein Aufklärungsbogen vom zuständigen Arzt lokal mit Patientendaten angereichert und über das interne WLAN der Einrichtung den Apps „Anamnese mobil“ und „Aufklärung mobil“ zur Verfügung gestellt.

Alle Daten, d.h. die Stammdaten des Patienten, alle Fragen und Antworten der Anamnese sowie eingriffs-spezifische Informationen (alle im Folgenden als „Anamnese-Daten“ bezeichnet) werden mit AES-128 verschlüsselt und in der Datenbank der lokalen ECP-Installation abgelegt. Zu keinem Zeitpunkt werden die Daten über das Internet an Thieme oder Dritte versendet. Die Daten werden im Rahmen des mobilen Workflows lediglich einrichtungsintern über das WLAN den oben benannten Apps zur Verfügung gestellt. Dabei kann frei konfiguriert werden, ob diese Daten im WLAN über http bzw. https ausgetauscht werden sollen, wobei auch die verwendeten Ports frei konfiguriert werden können. Dies wird bei der Erstinstallation des Systems festgelegt und kann jederzeit über die Setup-Datei für bestehende Installationen geändert werden.

Die Anamnese-Daten werden (sichtbar in der „Arbeitsliste Patienten“ der App „Aufklärung mobil“) standardmäßig in der Datenbank solange aufbewahrt, bis entweder der Datensatz in der Arbeitsliste manuell storniert wird oder aber der Datensatz der abgeschlossenen Aufklärung automatisiert nach einem definierten Zeitraum gelöscht wird. Dieser Zeitraum wird bei Neuinstallationen per Standard auf 4 Tage gesetzt und kann mandanten-spezifisch über die Zugriffsverwaltung geändert werden.

Neben diesem Auslieferungszustand gibt es noch die Möglichkeit, ECP anzuweisen, eine Anamnese-Historie für die Patienten zu speichern. In diesem Falle werden alle Anamnese-Daten zusätzlich neben der Speicherung für die Arbeitsliste ebenfalls mit AES-128 verschlüsselt in der Datenbank gespeichert. Diese Option ist aktiv freizuschalten, um das Prinzip der datenschutzfreundlichen Voreinstellungen gemäß EU Datenschutz-Grundverordnung („privacy-by-default“) sicherzustellen.

Die Speicherung der Anamnese-Historie bietet Patienten den Vorteil, dass bei erneuter Aufnahme/ Aufklärung desselben Patienten nach einem längeren Zeitraum wieder auf diese Daten zurückgegriffen werden kann, um umständliches Neuerfassen bereits bekannter Daten zu vermeiden. Die Daten der Anamnese-Historie werden standardmäßig fünf Jahre lang vorrätig gehalten. Zur Steuerung der Zugriffsmöglichkeit auf die Verwaltung der Anamnese-Historie gibt es in E-ConsentPro ein spezielles Recht, das beliebigen Nutzern (Usern der Software) zugeordnet werden kann und das Recht eröffnet, die Verwaltung zu nutzen.

In dieser Patientendaten-Verwaltung haben die dazu berechtigten Nutzer die Möglichkeit:

1) alle zu einem Patienten gespeicherten Daten aufzulisten,
2) diese Daten zu kopieren und so dem Patienten zur Verfügung zu stellen und
3) alle diese Daten patientenbezogen zu löschen.

Einmal auf diesem Wege gelöschte Patientendaten können nicht mehr angezeigt und/ oder genutzt werden. Um unbefugtem Zugriff grundsätzlich auszuschließen, geschieht die Identifikation der Patientendaten dabei über die Kombination der Patienten-ID, dem Vornamen, dem Nachnamen und dem Geburtsdatum. Ist eine dieser Informationen nicht bekannt, können keinerlei Daten angezeigt, exportiert oder gelöscht werden. Es ist nicht möglich, Daten mehrerer Patienten gleichzeitig zu verarbeiten.

Die einrichtungsinterne Patientendaten-Verwaltung verfügt über ein separates Logging, sodass nutzerspezifisch eingesehen werden kann, wer wann welche Daten angezeigt bzw. gelöscht hat.

Es gibt prinzipiell noch zwei andere Fälle, in denen Patientendaten in ECP mobile gespeichert werden, die hier der Vollständigkeit halber aufgezeigt werden sollen.

Verwenden Sie HL7, um Nachrichten von einem anderen System an ECP zu übergeben, so werden diese übergebenen Daten in der Datenbank, ebenfalls verschlüsselt mit AES-128, gespeichert. Diese sind so lange im Anamnese-Datensatz des Patienten vorhanden, wie dieser auch über die Arbeitsliste Patient erreichbar ist. Werden dort die Anamnese-Daten gelöscht, werden auch die zugehörigen HL7-Daten gelöscht.

Verwenden Sie die BDT/GDT- bzw. VDDS-Schnittstelle, so werden die zu übergebenden Daten von ECP ausgelesen und gespeichert, sobald die Bogenzuweisung erfolgt ist. Nach Abschluss der Aufklärung wird ggf. eine Antwortdatei erzeugt und in der Datenbank verschlüsselt abgespeichert. Sobald die Antwortdatei auf dem Client gespeichert werden konnte, wird sie wieder aus der Datenbank gelöscht.

Wie in jeder anderen Software gibt es auch in ECP ein Logging. Dieses Logging steht per default immer im Level „INFO“, sodass sichergestellt ist, dass keine Patientendaten geloggt und damit außerhalb der verschlüsselten Datenbank von ECP gespeichert werden. In besonderen Fällen und auf Wunsch des Kunden kann dieser Logging-Level unsererseits auf „DEBUG“ gestellt werden. Dabei ist sichergestellt, dass die Patientendaten lediglich anonymisiert in das Logging einfließen. Der Logging-Level „TRACE“, der ein vollständiges Logging aller Daten ermöglicht, ist ausschließlich für den internen Gebrauch mit Test-Patientendaten vorgesehen.

Online-Portal E-Consent

Werden Aufklärungsbögen über das Online-Portal E-Consent abgerufen, muss ein Kunde vor dem Ausdruck eines Bogens Name, Vorname und Geburtsdatum des Patienten eingeben. Zur Sicherstellung der Vollständigkeit eines ausgedruckten Bogens ist jede Einzelseite mit Patientennamen, Druck-Zeitpunkt, Bogentyp und Seitennummer im Format n von x gekennzeichnet. Dies vermeidet außerdem Verwechslungen von Einzelseiten verschiedener Patienten und dient zugleich der Copyright-Sicherung.

Die am Client erfassten Patientendaten werden im Rahmen einer Sitzung vom Kunden in verschlüsselter Form an E-Consent übertragen.

Zu keinem Zeitpunkt werden diese Daten von E-Consent in einer Datenbank gespeichert. Sie befinden sich ausschließlich temporär und nur in Form maschinenlesbarer Datenpakete (also keine Klartextdaten) im „flüchtigen“ Hauptspeicher. Es ist daher nicht möglich, von außen oder von einer anderen Sitzung aus auf die Patientendaten zuzugreifen. Nach dem Beenden der Sitzung (durch Ausloggen oder durch einen Timeout nach spätestens 30 Minuten) sind die Daten aus dem Hauptspeicher unwiederbringlich entfernt. Dies bedeutet, dass selbst dann keine Patientendaten mehr aus vergangenen Sitzungen verfügbar sind, wenn die Sitzung geschlossen wurde und derselbe Benutzer sich noch einmal bei E-Consent anmeldet.

Unsere Datenschutzbeauftragte ist an allen Phasen der Produkt-Entstehung beteiligt, vom Design bis zur abschließenden Anwendungsprüfung. Zusätzlich stehen wir in engem Dialog mit unseren Kunden, um die gesetzlichen Anforderungen sowohl als Produkthersteller als auch aus Sicht der Anwender und Nutzer betrachten und fortlaufend bewerten zu können. Auch die weiteren Anforderungen, die über das gewohnte Datenschutzniveau nach dem bisherigen Bundesdatenschutzgesetz von 2009 hinausgehen (BDSG-neu, TMG, ePrivacy-Verordnung etc.), sind für uns die selbstverständliche Fortschreibung unseres

gelebten Datenschutzes. Wir sind bestrebt, alle Anforderungen auch hier unverzüglich zu erfüllen, soweit und sobald dies in Abhängigkeit von der noch ausstehenden Positionierung der EU-Kommission bzw. der zuständigen Aufsichtsbehörden möglich ist.

Kontakt für weiterführende Fragen oder Anregungen zum Thema Datenschutz

Für weitere Fragen stehen wir Ihnen gern zur Verfügung und freuen uns besonders über produktive Anregungen, was wir aus Ihrer Sicht darüber hinaus anbieten können.

Zur optimalen Bearbeitung Ihrer Anliegen empfehlen wir Ihnen, den Erstkontakt mit unserer externen Datenschutzbeauftragten per E-Mail herzustellen:
Frau Blossey (datenschutz@thieme-compliance.de).