Datenschutz-Folgenabschätzung (DSFA)

Modul Versichertenstammdatenmanagement (VSDM)

Name des Erstellers dieser DSFA (z. B. Praxisinhaber):

_____

Erstellungsdatum dieser DSFA:

_____

I. Kontext

1. Überblick

Welche Verarbeitung ist geplant?

Die Telematikinfrastruktur (TI) soll gemäß § 291a SGB V alle Beteiligten im Gesundheitswesen, wie Ärzte, Psychotherapeuten, Krankenhäuser, Apotheken, Krankenkassen, miteinander vernetzen. Als erste Anwendung wird der „Versichertenstammdatenabgleich“ (VSDM) über die TI, unter Einbezug der elektronischen Gesundheitskarte (eGK), eingeführt. In weiteren Ausbaustufen sollen weitere Anwendungen, mit dem wesentlichen Ziel medizinische Informationen auszutauschen, hinzukommen.

Der Zugang zur TI erfolgt in der Praxis über den sog. TI-Konnektor. Dieser stellt ein virtuelles privates Netzwerk (VPN) zur TI her, welches eine verschlüsselte Kommunikation ermöglicht.

Welche Zuständigkeiten bestehen für die Verarbeitung?

Für die Verarbeitung von Daten innerhalb der Praxis ist grundsätzlich der Leistungserbringer der Verantwortliche. Für den Versichertenstammdatenabgleich wird die Praxis an die TI angeschlossen. Die DSK (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) vertritt gemäß Beschluss vom 12.09.2019, dass gemäß Artikel 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) eine Mitverantwortung der

gematik GmbH (Gesellschaft für Telematikanwendungen der Gesundheitskarte, im Folgenden: „gematik“) für die dezentralen TI-Komponenten, so auch den TI-Konnektor besteht.

Die hard- und softwaretechnische Spezifikation und Ausgestaltung liegen ausschließlich in der Verantwortung der gematik. Diese sind dem Leistungserbringer (Arzt) weitgehend unbekannt und in ihren Risiken daher nicht abschätzbar. Insbesondere lässt sich mangels Auskünften weder beurteilen, wie diese in das Praxisnetz integrierten Fremdkomponenten mit der Praxis-IT interagieren und auf diese einwirken können, noch wie Sicherheitsvorfälle in der Telematik über diese Geräte in die Praxis hinein wirken.

Der Versichertenstammdatenabgleich gehört nicht zu den originären datenverarbeitenden Anwendungen des Praxisbetriebs im medizinischen Sinne. Es handelt sich um eine administrative Anwendung der Krankenkassen, die aufgrund gesetzlicher Vorgaben in den Praxisbetrieb verlagert wurde (§§291, 291a SGB V).

Auch wenn die Fragen der datenschutzrechtlichen Mitverantwortung gemäß Art.26 DSGVO noch nicht geklärt sind, wird in Bezug auf die Entscheidung des Leistungserbringers über die Frage, ob der TI-Konnektor in Betrieb genommen werden soll bzw. ein installierter TI-Konnektor wieder außer Betrieb genommen werden soll, gleichwohl für den auf die Arztpraxis entfallenden Teil der Telematikinfrastruktur eine Datenschutzfolgenabschätzung durchgeführt.

Gibt es Normen oder Standards für die Verarbeitung?

Die rechtliche Grundlage für Art und Umfang der Verarbeitung von Gesundheitsdaten folgt aus den §§ 291, 291a SGB V.

2. Daten, Prozesse und Unterstützung

Welche Daten werden verarbeitetet?

Durch den Versichertenstammdatenabgleich (VSDM) werden einmalig pro Quartal die Daten auf der elektronischen Gesundheitskarte (eGK) mit dem VSDM-Dienst abgeglichen. Sollten Daten auf der eGK veraltet oder unvollständig sein, werden diese entsprechend aktualisiert.

In der ersten Rollout-Phase (VSDM) der Telematikinfrastruktur in 2019 sollen nach Angaben der gematik zunächst die gemäß § 291 SGB V auf der eGK gespeicherten Daten übertragen und abgeglichen werden. Hierbei handelt es sich um folgende Daten:

- Die Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die kassenärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat,

- den Familiennamen und Vornamen des Versicherten,
- das Geburtsdatum des Versicherten,
- das Geschlecht des Versicherten,
- die Anschrift des Versicherten,
- die Krankenversicherungsnummer des Versicherten,
- den Versichertenstatus, für Personengruppen nach § 264 Abs. 2 SGB V den Status der auftragsweisen Betreuung,
- den Zuzahlungsstatus des Versicherten,
- den Tag des Beginns des Versicherungsschutzes,
- bei befristeter Gültigkeit der elektronischen Gesundheitskarte das Datum des Fristablaufs.

In § 291 Abs. 2 Nr. 7 SGB V wird darüber hinaus auf den § 264 Abs. 2 SGB V verwiesen, also die Vorschrift „Versichertenstatus, für Personengruppen nach § 264 Abs. 2 der Status der auftragsweisen Betreuung“. Gemäß § 264 Abs. 4 S.3 und 4 SGB V gilt als Versicherungsstatus die Statusbezeichnung „Mitglied“, „Rentner“ oder „Familienversicherter“. Der Status der auftragsweisen Betreuung nach § 264 Abs. 2 kann die Werte „SGB XII“, „Asylbewerberleistungsgesetz“ und „Krankenhelfer“ haben.

Die tatsächlich auf der elektronischen Gesundheitskarte speicherbaren Daten zum Versichertenstatus ergeben sich aus untergesetzlichen Normen, namentlich aus dem „Fachkonzept Versichertenstammdatenmanagement“ der gematik und aus der „technischen Anlage zu Anlage 4 Bundesmantelvertrag-Ärzte (BMV-L)“. Gesetzliche Grundlage für den Erlass der technischen Normen sind § 291 b Abs.1 Nr.2 und §§ 291 Abs.3, 87 Abs.1 S.2 SGB V. In den beiden technischen Spezifikationen ist unter anderem geregelt, dass auf der eGK ein „DMP-Kennzeichen“ gespeichert wird, das folgende Werte haben kann:

- Diabetes Mellitus Typ 2,
- Brustkrebs,
- Koronare Herzkrankheit,
- Diabetes Mellitus Typ 1,
- Asthma Bronchiale,
- COPD,

siehe: „Fachkonzept Versichertenstammdatenmanagement“, Seite 43, abrufbar unter https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Basis-Rollout/Fachanwendungen/gematik_VSD_Fachkonzept_VSDM_V270.pdf.

Es ist auch fraglich, ob durch untergesetzliche Normen ein derartiger Datentransfer stattfinden darf.

Wie verläuft der Lebenszyklus von Daten und Prozessen?

- Die VSD (Versichertenstammdaten) werden online abgefragt.
- Aktualisierungsbedarf wird festgestellt.
- Aktualisierungsanfrage erfolgt beim Kostenträger.
- Übermittlung der VSD erfolgt.

Bewertung: Die technische Umsetzung der Ergänzung und Aktualisierung von VSD stellt sich bisher als nicht ausreichend transparent dar. Hier ist zwingend erforderlich, dass die gematik eine klare und nachvollziehbare Darstellung der Prozesse vorlegt.

Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung?

Die Datenverarbeitung in meiner Praxis erfolgt durch die folgenden Betriebsmittel:

- Konnektor – fremdkontrollierte Komponente mit dem Praxisinhaber unbekannter Funktion und Sicherheitsniveau;
- elektronisches Kartenterminal – fremdkontrollierte Komponente mit dem Praxisinhaber unbekannter Funktion und Sicherheitsniveau;
- Praxis-Netzwerk als reines Transportnetz;
- Internet als Transportnetz für ein fremdkontrolliertes TI-VPN mit dem Praxisinhaber unbekannter Funktion und Sicherheitsniveau;
- dem Praxisinhaber unbekannte, fremdkontrollierte Komponenten unbekannter Funktion und Sicherheitsniveaus in der TI und unbekannten sogenannten „Bestandsnetzen“;
- möglicherweise in unbekanntem Umfang, mit dann fremdkontrollierter Funktion und Sicherheitsniveau, das Praxisverwaltungssystem (PVS alias AIS).

Bewertung: Dies stellt, auch aus gesetzessystematischer Sicht, einen erheblichen und ungerechtfertigten Bruch dar, da der Praxisinhaber – mindestens auch Verantwortlicher i. S. d. DSGVO – Herr über die Daten und deren Verarbeitung ist und bleiben muss.

Grundlegende Prinzipien

1. Verhältnismäßigkeit und Notwendigkeit

Sind die Verarbeitungszwecke eindeutig definiert und rechtmäßig?

Die Verarbeitungszwecke sind ausreichend definiert. Im Wesentlichen sind die Verarbeitungszwecke in §§ 291, 291a SGB V geregelt.

Aufgrund welcher Rechtsgrundlage erfolgt die Verarbeitung?

Rechtsgrundlage ist Art. 9 Abs. 2 lit. i, 1. Hs. DSGVO i. V. m. §§ 291, 291a SGB V.

Sind die erhobenen Daten erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?

Die erhobenen Daten für die Verarbeitung sind gesetzlich vorgegeben.

Sind die Daten korrekt und auf dem neuesten Stand?

Der Datenabgleich der Versichertenstammdaten erfolgt über die TI.

Bewertung: Da der Datenabgleich der Krankenkassen über die TI abgeglichen wird, kann die Praxis die Richtigkeit und Aktualität der Daten selber nicht bewerten.

Welche Speicherdauer haben die Daten?

Die Speicherdauer in der TI oder bei den Krankenkassen kann durch den Praxisinhaber nicht bewertet werden.

2. Maßnahmen zum Schutz der Persönlichkeitsrechte der betroffenen Personen

Wie werden die betroffenen Personen über die Verarbeitung informiert?

Wir gehen davon aus, dass aufgrund der gesetzlichen Regelung eine Informationspflicht nicht besteht. Bei gemeinsam Verantwortlichen (Art.26 DSGVO) ist jedoch gerade die

Regelung der Aufgabenverteilung, so auch der Erfüllung der Betroffenenrechte, ein wichtiger Aspekt. An einer solchen Regelung bzw. Vereinbarung fehlt es bislang.

Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?

Einer Einwilligung bedarf es nach Art. 6 Abs. 1 lit. c und Abs. 3 DSGVO bzw. Art. 9 Abs. 2 lit. i, 1. Hs. DSGVO i. V. m. §§ 291, 291a SGB V nicht.

Wie können Betroffene ihre Rechte auf Auskunft und Datenübertragbarkeit ausüben?

Die Erfüllung der Betroffenenrechte ist derzeit nicht gewährleistet. Hinsichtlich des VSDM ist die Praxis weder auskunftsfähig noch handlungsfähig, hierfür müsste die gematik sich im Zuge einer Joint-Controllership-Vereinbarung gemäß Art.26 Abs.1 S.2 DSGVO verantwortlich erklären oder eine solche Aufgabenverteilung müsste gemäß Art.26 Abs.1 S.2 DSGVO durch Rechtsvorschriften geregelt werden.

Wie können betroffene Personen ihr Recht auf Berichtigung und Löschung (Recht auf Vergessenwerden) ausüben?

Auch hierzu gelten die vorstehenden Ausführungen. Die Erfüllung der Betroffenenrechte ist derzeit nicht gewährleistet. Hinsichtlich des VSDM hat die Praxis keine Berichtigungs- oder Löschungsmöglichkeiten.

Wie können betroffene Personen ihre Rechte auf Einschränkung oder Widerspruch der Verarbeitung ausüben?

Auch hierzu gelten die vorstehenden Ausführungen. Die Erfüllung der Betroffenenrechte ist derzeit nicht gewährleistet. Die Praxis kann, mangels Kenntnisse zum Verarbeitungsvorgang, keine Prüfung im Falle eines Widerspruchs vornehmen und mangels Zugriffsrechte, auch den Verarbeitungsvorgang nicht einschränken (mit Ausnahme einer vollständigen Außerbetriebnahme).

Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?

Soweit die Arztpraxis für die Inbetriebnahme des TI-Konnektors und dessen Wartung einen Dienstleister einsetzt und dieser eine theoretische Zugriffsmöglichkeit auf Daten erhält, wird eine Auftragsverarbeitungsvereinbarung gemäß Art.28 DSGVO abgeschlossen.

Soweit Datenübermittlungen in Länder außerhalb der Europäischen Union stattfinden, werden die Daten angemessen geschützt?

Grundsätzlich findet in der Arztpraxis selbst keine Übermittlung von personenbezogenen Daten außerhalb der EU bzw. des EWR wissentlich statt. Der Praxisinhaber hat keinerlei Kenntnis oder Kontrolle darüber, ob von anderen Beteiligten der Telematikinfrastruktur (z.B. gematik oder Krankenversicherungen) im Rahmen des VSDM personenbezogene Daten außerhalb der EU bzw. des EWR übermittelt werden.

Bewertung: Die Kenntnis über Fragen der geografischen Reichweite von Datenübermittlungen im Rahmen der technischen Umsetzung der TI entzieht sich der Kenntnis der Praxisbetreiber.

Daher ist der technische Dienstleister gematik gehalten und aufzufordern, die Datenübermittlungsprozesse insgesamt – insbesondere auch in Bezug auf die geografische Reichweite – transparent und nachvollziehbar zu dokumentieren und eine Garantie abzugeben, dass die Datenübermittlung nur dann erfolgt, wenn aus technischer und rechtlicher Sicht eine ausreichende Datensicherheit gewährleistet ist (bei Datenübermittlungen ins Ausland ist sicherzustellen, dass die im Zielland geltenden Regelungen einen vergleichbaren Schutzgehalt wie die DSGVO vermitteln).

II. Risiken

1. Geplante oder bestehende Maßnahmen

Bis zur Umsetzung der vorgenannten Maßnahmen und Klärung der datenschutz- und sicherheitsrelevanten Fragen durch die gematik sowie weiterer Verantwortliche, stellt sich das Aufschieben der Inbetriebnahme bzw. die Abschaltung des Konnektors für den Praxisbetreiber – unter Berücksichtigung des folgend dargestellten Bedrohungspotentials – als gerechtfertigte Maßnahme dar.

Was sind die Hauptbedrohungen, die zu einem Risiko führen könnten?

Zugriff auf Patientendaten im Praxisverwaltungssystem.

Es handelt sich um hoch schutzbedürftige medizinische Daten.

Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Ihr Bekanntwerden kann die gesellschaftliche und wirtschaftliche Stellung des Betroffenen erheblich schädigen. Für potentielle Arbeitgeber, Versicherer und sonstige Vertragspartner sind die Gesundheitsdaten eines Menschen eine wertvolle Information. Aber nicht nur der Patient selbst ist betroffen: Medizinische Daten treffen teils schon heute, und im Rahmen des Forschungsfortschritts wahrscheinlich zunehmend, auch Aussagen zu gesundheitlichen Risiken von engeren Verwandten des Betroffenen, so dass auch deren gesellschaftliche und wirtschaftliche Stellung geschädigt werden kann.

Was sind die Risikoquellen?

- Unmittelbare Einwirkung aus der Telematik-Infrastruktur, etwa durch Konnektorfunktionalität (bspw. Layer-2-Tunneling) oder Versagen der Sicherheitsfunktionen im Konnektor (bspw. Paketfilterung, Fernzugangabsicherung).
- Mittelbar, indem fehlerhafte oder böswillig manipulierte Versichertenstammdaten eine Fehlfunktion im Praxisverwaltungssystem auslösen, die einem Angreifer Kontrolle über das System verschafft (bspw. ein Buffer-Overflow, SQL-Injection, etc.).
- Unmittelbare Fehlkonfiguration oder -installation von TI-Komponenten in der Praxis, etwa bei Erst- oder Ersatzinstallationen sowie evtl. Updates, insbesondere im Rahmen der vorgesehenen Fernwartung.
- Mittelbare Fehlkonfiguration in der Praxis-IT, etwa bei Erst- oder Ersatzinstallationen sowie Updates und Fehlerbehebung. Erfahrungsgemäß besteht das Risiko, dass unabgestimmt andere sicherheitsrelevante Komponenten der Praxis-IT zur Fehlersuche deaktiviert oder entschärft werden und entweder die Rücknahme dieser sicherheitsrelevanten Änderungen vergessen wird oder die Änderungen als erfolgreiche und erforderliche Fehlerbeseitigung dargestellt werden.

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Die Nichtanwendung bzw. die Nichtinstallation des TI-Konnektors schaltet das Risiko verlässlich aus.

Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Das Schadensausmaß kann für einzelne Patienten (und Anverwandte) erheblich sein.

Die Nichtanwendung bzw. die Nichtinstallation des TI-Konnektors schaltet das Risiko aus.

Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?

Aufgrund der schlechten Informationsanlage – etwa hinsichtlich praktischer Sicherheitstests (Pen-Tests) an den Komponenten – und der mangelnden Mitwirkung der gematik, kann die Eintrittswahrscheinlichkeit nicht sinnvoll eingeschätzt werden.

2. Unerwünschte Veränderung von Daten

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Unbemerkte Manipulation oder Löschung von Patientendaten im Praxisverwaltungssystem.

Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Wird die Behandlung auf unbemerkt manipulierte Patientendaten gestützt und werden gelöschte Daten bei der Behandlung nicht beachtet, kann es in Einzelfällen zu schwerwiegenden Fehlbehandlungen, mit gravierenden gesundheitlichen Folgen kommen.

Was sind die Risikoquellen?

s.o.

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

s.o.

Die Nichtanwendung bzw. die Nichtinstallation des TI-Konnektors schaltet das Risiko aus.

Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Da es zu gravierenden gesundheitlichen Folgen kommen kann, wird das Schadenspotential als maximal/katastrophal eingestuft.

Die Nichtanwendung bzw. die Nichtinstallation des TI-Konnektors schaltet dieses Risiko aus.

Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?

s.o.

3. Datenverlust

Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Ein Datenverlust – sei es die tatsächliche dauerhafte Nicht-Verfügbarkeit oder die erkannte Manipulation – führt zum Verlust von Behandlungshistorie.

Die jüngste Historie und aktuelle Medikation sollte allerdings in den allermeisten Fällen auf mehreren Wegen rekonstruierbar sein.

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

s.o.

Was sind die Risikoquellen?

s.o.

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Die Nichtanwendung bzw. die Nichtinstallation des TI-Konnektors schaltet das Risiko aus.

Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Die Nichtanwendung bzw. die Nichtinstallation des TI-Konnektors schaltet das Risiko aus. Für den einzelnen Patienten ergeben sich keine Nachteile.

Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?

s.o.

III. Aktionsplan

1. Grundlegende Prinzipien

Es ist kein Aktionsplan festgelegt.

Der Praxisinhaber hat in der Praxis, mit Ausnahme der Entscheidung über die Nichtvornahme der Installation bzw. über eine Außerbetriebnahme, keinerlei Kontrolle oder Einwirkungsmöglichkeiten auf die TI-Komponenten.

Er hat ebenfalls keinerlei Kontrolle oder Einwirkungsmöglichkeiten auf den Betrieb der TI im Allgemeinen sowie das VSDM im Speziellen.

2. Bestehende oder geplante Maßnahmen

Der Betrieb der dezentralen TI- Komponente "Konnektor" und damit die Einbindung der Praxis in die TI wird nicht begonnen bzw. durch Abschalten des Konnektors ausgesetzt ("Aussetzen der Verarbeitung") bis eine der folgenden Bedingungen eintritt:

1. Die gematik erklärt ihre Mitverantwortung als "Joint Controller" für den TI-Konnektor im Praxisbetrieb entsprechend dem Beschluss der DSK vom 12.09.2019 und kommt ihren Mitwirkungspflichten nach, sodass eine Joint-Controllership-Vereinbarung gemäß Art.26 Abs.1 S.2 DSGVO abgeschlossen werden kann.

2. Die Aufgabenverteilung zwischen den gemeinsam Verantwortlichen wird gemäß Art.26 Abs.1 S.2 DSGVO durch Rechtsvorschriften festgelegt und stellt die alleinige Verantwortung der gematik für den Betrieb von Konnektor, Kartenterminal und das VSDM, sowie für alle Sicherheitsvorfälle und Datenschutzverletzungen, für die eine Beteiligung von TI-Komponenten und -Funktionen nicht sicher ausgeschlossen werden kann, fest.

3. Risiken

Die durch die mangelnde Mitwirkung der gematik notwendige Nichtanwendung bzw. Nichtinstallation des Konnektors birgt folgende Risiken:

- VSD von Patienten werden nicht aktualisiert. Für die Sicherheit der Behandlung dieser Patienten und für deren Daten geht von dieser Maßnahme keine Gefahr aus.
- Es drohen Honorareinbußen für die Praxis aufgrund der Sanktionsregelung gemäß § 291 Abs.2b S.14 SGB V. Da die Notwendigkeit des Aufschiebens der Inbetriebnahme bzw. der Abschaltung des TI-Konnektors durch die fehlende Mitwirkung der gematik verursacht wurde, bleiben Regressansprüche gegen die gematik vorbehalten.