

TI-Hinweise 3

August 2020

Inhalt

1.	Einleitung.....	3
2.	Anwendungen.....	4
2.1.	Gesetzlich festgelegte Anwendungen	4
2.1.1.	Versichertenstammdatenmanagement (VSDM)	4
2.1.2.	Notfalldatenmanagement (NFDm).....	4
2.1.3.	Elektronischer Medikationsplan und Daten für die Arzneimitteltherapiesicherheitsprüfung (eMP/AMTS)	5
2.1.4.	Elektronische Patientenakte (ePA)	5
2.1.5.	eRezept	6
2.2.	Weitere Dienste und Anwendungen	6
2.2.1.	Elektronische Fallakte (EFA)	6
2.2.2.	Kommunikation im Medizinwesen (KIM).....	7
2.2.3.	auf der TI aufbauende Anwendungen	7
3.	TI-Komponenten und Begriffe.....	9
3.1.	Konnektor	9
3.2.	Kartenterminal	9
3.3.	VPN-Zugangsdienst	10
3.4.	Institutionskarte (SMC-B).....	11
3.5.	Heilberufsausweis (HBA).....	12
3.6.	Anpassung Primärsysteme	13
4.	Finanzierungsvereinbarung	14
5.	Übersicht über die Fristen.....	15
5.1.	Handhabung Fristen	16

1. Einleitung

Diese Hinweise enthalten Informationen zur Einführung des Versichertenstammdatenmanagements und weiterer Anwendungen, die über die Telematikinfrastruktur (TI) bereitgestellt werden, im Krankenhaus. Dabei wird ein Gesamtkonzept verfolgt mit dem Ziel, das gesamte Krankenhaus in die Betrachtung einzubeziehen und nicht nur einzelne Bereiche wie z.B. Ambulanzen. Abgewichen werden muss von dem Gesamtkonzept voraussichtlich, weil die gesetzlichen vorgegebenen Termine teilweise eine Planung und Ausstattung notwendig machen, die später um Software-Updates ergänzt wird. Dieser möglicherweise gestufte Prozess sollte jetzt in einem TI-Einführungsprojekt vom Krankenhaus bzw. dem Träger, ggf. mit dem IT-Dienstleister, bis hin zur Einführung der elektronischen Patientenakte (ePA) geplant und ausgeführt werden.

2. Anwendungen

2.1. Gesetzlich festgelegte Anwendungen

Neben der reinen „TI“-Infrastruktur bestehend aus dem zentralen, alles verbindenden Netz, dezentralen Komponenten wie Konnektoren und Kartenterminals, mit verschlüsselten Verbindungen, kryptografischen Identitäten und passendem Verzeichnisdienst, ist über die TI eine zunehmende Zahl von Anwendungen erreichbar, die im folgenden Text beschrieben werden – jeweils mit dem Schwerpunkt auf deren Einführung im Krankenhaus.

Alle Anwendungen setzen eine Anpassung der jeweiligen Systeme voraus – hierbei muss es sich nicht immer um das medizinische Primärsystem handeln, sondern es müssen jeweils die Systeme angepasst werden, die für die entsprechende Aufgabe verwendet werden. Die gematik bietet Herstellern die Möglichkeit an, einen Konnektor-Simulator zu nutzen und erlaubt so einen Konformitätstest. Zusätzlich gibt die gematik zu Anwendungen Implementierungsleitfäden heraus. Darüber hinaus hat die gematik aber keinen Einfluss auf die Implementierung in den Primärsystemen – hier muss jedes Krankenhaus die angepasste Software der jeweiligen Hersteller auf Eignung für die individuellen Anforderungen und auf die Einbindung in die Behandlungsprozesse prüfen.

2.1.1. Versichertenstammdatenmanagement (VSDM)

Vermittelt vom Konnektor wird eine direkte verschlüsselte Verbindung von der eGK zu den Systemen des Versichertenstammdatenmanagements der Krankenkassen aufgebaut, von dort neue Inhalte auf die eGK übernommen und den Primärsystemen bereitgestellt. Der Konnektor und das Primärsystem können so eingestellt werden, dass bei jedem Stecken der eGK nicht nur anhand der Zertifikate und der Sperrlisten online geprüft wird, ob es sich um eine gültige eGK handelt, sondern auch bei der Kasse nachgefragt wird, ob evtl. eine Aktualisierung für diese Karte vorliegt. Diese Aktualisierung kann eine Sperrung veralteter/verlorener eGK sein oder eine Adressänderung nach einem Umzug. Namensänderungen können nicht online aktualisiert werden, da durch den Aufdruck des Namens immer die Karte ausgetauscht werden muss.

In den vertragsärztlichen Bereichen ist die Online-Prüfung auch im Krankenhaus verpflichtend und ein in diesem Prozess erzeugter Prüfnachweis muss mit der Abrechnung übermittelt werden. Das Ausbleiben der Prüfung ist mit einer Sanktion belegt und nur mit diesem Prüfnachweis kann der KV bewiesen werden, dass die notwendige Ausstattung vorhanden ist. Um den Prüfnachweis entgegen nehmen zu können muss das eingesetzte Primärsystem angepasst sein.

In der stationären Versorgung, die im Gegensatz zur vertragsärztlichen Versorgung nicht zum Online-VSDM verpflichtet ist, kann es sinnvoll sein, die VSDM-Aktualisierung durchzuführen, da man so z.B. Adressänderungen ohne händische Eingabe in die Systeme übernehmen kann und zusätzlich sicherstellt, mit der aktuellen eGK und darauf verfügbaren Daten zu arbeiten.

2.1.2. Notfalldatenmanagement (NFDM)

Die Notfalldaten können als signierte Datei auf die eGK geschrieben und von dieser ausgelesen werden. Bei einer Aktualisierung wird der vorherige Datensatz auf der eGK mit der geänderten Fassung überschrieben. Um diese Anwendung in ein Primärsystem zu integrieren muss dieses insbesondere eine Anzeige und eine Eingabe für Notfallda-

ten implementieren. Bei der Eingabe können Komfortfunktionen dafür sorgen, dass bestimmte Felder mit Daten aus der internen Patientenakte automatisch oder nach Bestätigung durch die erfassende Person übernommen werden. Auch umgekehrt wäre es wünschenswert, wenn Informationen aus dem CAVE-Bereich in die interne Patientenakte oder einen Anamnesebogen übernommen würden.

Die Funktion zum Lesen der Notfalldaten muss evtl. in mehreren Systemen verfügbar sein, wenn z.B. auf den Intensivstationen oder im Schockraum andere Systeme zum Lesen der eGK verwendet werden, als bei einer ärztlichen Aufnahme auf den Stationen.

Es muss sichergestellt werden, dass im System hinterlegt ist, wer zum Lesen der Notfalldaten berechtigt ist, und der Lesevorgang protokolliert wird.

2.1.3. Elektronischer Medikationsplan und Daten für die Arzneimitteltherapiesicherheitsprüfung (eMP/AMTS)

Auf der eGK kann ein elektronischer Medikationsplan gespeichert werden, deren Inhalt in der ersten Umsetzungsstufe dem bundesweiten Medikationsplan entspricht. Die darin hinterlegten Daten können auch für eine elektronische Prüfung im Rahmen der Arzneimitteltherapiesicherheit verwendet werden.

An welchen Arbeitsplätzen der Medikationsplan eingelesen wird, ergibt sich aus den Abläufen der Aufnahme. Eine sinnvolle Variante kann das Einlesen des Medikationsplans direkt bei der Aufnahme sein, dann muss allerdings sichergestellt werden, dass rein administrative Aufnahmekräfte keinen Zugang zu den medizinischen Daten erhalten, sondern der eMP zur Verwendung und im Auftrag des Arztes direkt in die medizinische Dokumentation übernommen wird.

Das Erstellen eines Medikationsplans kommt im Rahmen der Entlassung in Frage.

2.1.4. Elektronische Patientenakte (ePA)

Kern der gesetzlichen Festlegungen zu der elektronischen Patientenakte (ePA) ist, dass der Patient die Hoheit über die Daten hat und jederzeit die Zugriffsrechte ändern oder einzelne Dokumente löschen kann.

Daten aus der ePA können im Krankenhaus insbesondere bei der initialen Anamnese hilfreich sein. Sollte das Krankenhaus noch nicht zum Zugriff auf die ePA berechtigt sein, ist auf eine Adhoc-Berechtigung im Krankenhaus mit Stecken der eGK und Bestätigung des Patienten möglich. Für die eigentlichen Zugriffe auf die ePA, d.h. das Abrufen oder das Einstellen von Dokumenten, werden keine Kartenterminals und insbesondere keine Heilberufsausweise benötigt. Dokumente, die in die ePA eingestellt werden, müssen dazu nicht signiert werden. Datensätze wie die Notfalldaten, die gemäß gesetzlichen Anforderungen mit dem HBA signiert werden, können auf Wunsch des Patienten in dieser Form in die ePA übernommen werden.

Aus der ePA abgerufene Daten sollten in die Primärdokumentation übernommen werden, um bei einer Änderung der Zugriffsrechte in der ePA oder bei einer Entfernung von Dokumenten aus der ePA durch den Patienten keine Nachweisprobleme entstehen zu lassen. Zum anderen können auf Wunsch des Patienten zu der oder nach der Entlassung Dokumente in die ePA geschrieben werden.

Sobald Sensoren bzw. Beobachtungs- oder Messgeräte in der Lage sind im Auftrag des Patienten Daten automatisch in die ePA zu schreiben, ist ein großes Standardisierungsproblem des Tele-Monitoring gelöst und die ePA kann im Bereich des Tele-Monitoring besondere Bedeutung entfalten. Aus Sicht des Krankenhauses spielt es

dann keine Rolle mehr, welches Gerät für ein Verfahren genutzt wird – es wird nur noch der Lesezugriff auf die ePA benötigt, um die Daten zu empfangen. Derzeit ist offen, welche Relevanz solche Szenarien entwickeln, oder ob die Interaktion mit Digitalen Gesundheitsanwendungen (DiGAs) der Patienten mehrheitlich z.B. über Webbrowser abgebildet wird.

Zu der Anwendung ePA werden voraussichtlich zusätzliche Umsetzungshinweise als eigenes Dokument bereitgestellt.

2.1.5. eRezept

Die Übermittlung ärztlicher Verordnungen (eRezept) gemäß § 360 Abs. 2 und 3 SGB V in der Bundestags-Beschlussfassung zu dem Patientendaten-Schutz-Gesetz ist im Krankenhaus dort umzusetzen, wo Verordnungen ausgestellt werden, die in den regulären Abrechnungsprozess nach § 300 SGB V Eingang finden müssen. Dies betrifft neben dem Entlassmanagement, mit der Erstellung von Verordnungen für die Anschlussmedikation, die Onkologie mit der Verordnung von Zytostatika, ggf. i.V.m. der Verordnung von parenteraler Ernährung, und der entsprechenden Einbindung der KH-Apotheke in den elektronischen Abrechnungsprozess spätestens ab 1.1.2022.

Detailfestlegungen zu dem eRezept wird die gematik mit einem Release 4.0.1 in der zweiten Jahreshälfte 2020 finalisieren. Dann lässt sich auch ermitteln, welche Maßnahmen im Krankenhaus zur Umsetzung des eRezepts, ergänzend zu der ohnehin anstehenden TI-Anbindung, notwendig sind. Beachten Sie bitte die dazu im Jahresverlauf bereitgestellten Informationen ihrer Krankenhausgesellschaft.

2.2. Weitere Dienste und Anwendungen

Grundsätzlich ist die TI offen für weitere Anwendungen und aus Sicht der DKG ist dies auch dringend notwendig, damit das Thema sichere Übermittlung von Informationen in möglichst einfacher Art und Weise abgewickelt werden kann.

Bisher wurden zwei zusätzliche Dienste implementiert: Das sichere Internet (SIS) und die Tunnelung von Bestandsnetzen. Letzteres verhindert, dass Anwendungen, die nicht direkt in die TI migriert werden und nur über schon vorher existierende „Bestandsnetze“ verfügbar sind, einen zweiten VPN-Zugang benötigen. Die Bestandsnetze werden mit einem Gateway an die TI angeschlossen und dort betriebene Anwendungen können dann vom Krankenhaus über den Konnektor erreicht werden.

2.2.1. Elektronische Fallakte (EFA)

Während der Patient bei der ePA die volle Kontrolle über die Inhalte hat und die ePA in vielen Szenarien gut anwendbar ist, lassen sich damit keine übergreifenden Versorgungsprozesse abbilden, bei denen Ärzte sich auf das Vorhandensein von vereinbarten Informationen verlassen müssen. Genau in diesen Szenarien kommt seit einiger Zeit die elektronische Fallakte (EFA) zum Einsatz.

Die EFA wird derzeit, begleitet von einem Projekt der gematik, beispielhaft in die TI migriert. Der EFA-Provider benötigt dabei eine Bestätigung der gematik, dass seine Anwendung die TI nicht gefährdet, und die EFA-Dienste-Server müssen über die TI erreichbar gemacht werden. Ist dies vollzogen, müssen die Berechtigungen zum Zugriff auf die einrichtungsübergreifenden elektronischen Fallakten perspektivisch nicht mehr über Listen von Zugriffsberechtigten bei den EFA-Providern gepflegt werden.

Um die Institutionsberechtigung in der TI verfügbar zu machen wurde ein Security-Token-Service unter dem Namen tokenbasierte Authentifizierung (TB-Auth) in die Spezifikationen der gematik integriert und kann dort nicht nur für die EFA sondern für alle Diensttypen verwendet werden, die eine sichere Autorisation einer Institution bei gleichzeitiger Identifikation einer dort berechtigten Person benötigen. Für die Berechtigungsvergabe können Krankenhäuser und andere Leistungserbringer ihre Institutionsidentitäten in der TI verwenden und damit die korrekte Anmeldung von Ärzten und Gehilfen am Primärsystem bestätigen. Dazu wird zukünftig auf das zentrale Verzeichnis der TI zurückgegriffen. Der EFA-Dienst-Betreiber kann die Zugriffsberechtigung über die Dienste der TI validieren. Die organisatorischen Prozesse der Berechtigungsvergabe werden deutlich vereinfacht.

2.2.2. Kommunikation im Medizinwesen (KIM)

Die Kommunikation im Medizinwesen (KIM), ehemals Kommunikation Leistungserbringer (KOM-LE) genannt, wurde als Anwendung für den sicheren Austausch adressierter Nachrichten zwischen Leistungserbringern spezifiziert. In diese Kommunikation ist der Patient in der Regel nicht direkt eingebunden.

KIM ist technisch gesehen ein Dienst für verschlüsselte E-Mails, wobei unterschiedliche Provider diesen Dienst in der TI anbieten. Krankenhäuser können KIM bei einem zugelassenen Provider einkaufen und dann in die bestehenden Systeme zum Versenden von Nachrichten integrieren. KIM ist so spezifiziert, dass ein gebräuchlicher E-Mail-Client über Standard-E-Mail-Schnittstellen Nachrichten austauschen kann, die dann vom KIM-Client-Modul im Hintergrund mit dem Konnektors verschlüsselt und signiert an den Provider zur Zustellung übermittelt werden. So können bestehende E-Mail-Anwendungen verwendet werden, ohne dass diese angepasst werden müssen. Alternativ wird von der gematik die Möglichkeit ausspezifiziert, die Funktionalität des KIM-Client-Moduls direkt in das Primärsystem zu integrieren, so dass ein KIS-Angebot mit „eingebautem KIM“, ohne separates KIM-Client-Modul, denkbar wird.

KIM wurde für die Übertragung von Arztbriefen entwickelt, die verschlüsselt auf die adressierte Institution versendet werden und dazu mittels einer Institutionssignatur beim Versand integritätsgeschützt werden. Die Arztbriefe müssen dabei nicht mit einem HBA signiert sein. KIM funktioniert einwandfrei ohne HBA, der z.B. nur dann zum Einsatz kommt, wenn ein Arztbrief in der vertragsärztlichen Versorgung über Gebührensatz abgerechnet werden soll, die eine qualifiziert elektronische Signatur mit dem HBA vorsehen.

KIM wirdzunehmende Bedeutung erlangen, wenn weitere Anwendungen des Gesundheitswesens zukünftig verstärkt über KIM abgewickelt werden, z.B. die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) und das elektronische Meldeverfahren für meldepflichtige Infektionskrankheiten (DEMIS). Für die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) ist die Verwendung von KIM als Transportwegfestgeschrieben.

2.2.3. auf der TI aufbauende Anwendungen

In den vergangenen Jahren konnten neu etablierte Anwendungen regelmäßig nicht auf der Telematikinfrastruktur aufbauen, weil der Rollout bei den Leistungserbringer-Zielgruppen der jeweiligen Anwendungen noch nicht abgeschlossen war. Diese Situation wandelt sich absehbar. Mit der Umsetzung der vorgenannten Anwendungen in den Krankenhäusern, in Arztpraxen und Zahnarztpraxen sowie Apotheken und mit der Erweiterung der TI um Reha-Kliniken und weitere Berufsgruppen, z.B. Hebammen, mit dem Abschluss des Gesetzgebungsverfahrens zum Patientendaten-Schutz-Gesetz,

wird die Telematikinfrastruktur zunehmen zu einer Plattform, an die weitere Anwendungen nutzbringend angebunden werden können.

Die TI kann als reines Transportverfahren für die Daten von weiteren Anwendungen verwendet werden. Die TI „kann“ jedoch mehr. Mit ihren kryptografischen Identitäten und Verschlüsselungszertifikaten, die jedem TI-Teilnehmer zur Verfügung stehen, können Anwendungen, die Authentisierungsverfahren oder Verschlüsselung benötigen, diese TI-Komponenten verwenden.

Wir gehen davon aus, dass in Zukunft zunehmend Anwendungen auf der TI aufbauen werden, wie dies heute bereits mit der eAU zu beobachten ist, die über KIM durch die TI transportiert wird.

3. TI-Komponenten und Begriffe

Die folgenden Betrachtungen beleuchten nicht die gesamte TI. Der Schwerpunkt liegt auf den Teilen, die für das Krankenhaus relevant sind, den sogenannten dezentralen Komponenten.

Auf <https://fachportal.gematik.de/zulassungen/online-produktivbetrieb/> veröffentlicht die gematik Zulassungslisten, die vom Krankenhaus bei der Auswahl passender zu beschaffender Konnektoren, Kartenterminals usw. herangezogen werden können. Soweit vorhanden stehen hinter den Zulassungsmerkmalen weitere Informationen zu den einzelnen Produkten bereit, die angetippt bzw. ausgeklappt werden können, um z.B. Hinweise zu erhalten, ob ein Konnektor für den Einbau in einen 19-Zoll Serverschrank geeignet ist.

3.1. Konnektor

Der Konnektor durchläuft in jeder Entwicklungsstufe, der eine Produkttypversion der gematik zugeordnet ist, ein Zulassungsverfahren. Konnektoren werden seit einiger Zeit in der Produkttypversion 2 (PTV2) angeboten. Derzeit laufen Feldtests mit PTV3-Konnektoren, die neben der qualifizierten elektronischen Signatur mit dem HBA die Anwendungen NFDM und eMP sowie KIM (und damit die eAU) unterstützen. Die folgende Produkttypversion PTV4 wird zusätzlich die ePA unterstützen. Um einen Konnektor im Betrieb von einer Produkttypversion zur nächsten zu aktualisieren muss ein Software-Update in den Konnektor eingespielt werden. Ein Austausch des Konnektors ist in der Regel nicht erforderlich, wenn der Hersteller das Software-Update bereitstellt.

Im Konnektor wird vom Krankenhaus ein Informationsmodell hinterlegt, das die korrekte Zuordnung von Primärsystemen und Kartenterminals zu Arbeitsplätzen und Mandanten festlegt. Das Informationsmodell kann in jedem Konnektor vom Administrator über ein Web-Interface mit einem üblichen Webbrowser gepflegt werden. Dieser „händische“ Ansatz stößt bei größeren Einrichtungen an Grenzen, wenn die Kombinationszahl der Zuordnungen zu weit ansteigt. Um diesem Problem zu begegnen, wurden Rechenzentrums-konnektoren entwickelt, die sich in einen 19-Zoll Serverschrank im Rechenzentrum einbauen lassen und für die eine Administrationssoftware angeboten wird, die einen Import von Arbeitsplatzkonfigurationen in den Konnektor unterstützt und die ggf. Daten aus bestehenden IT-Verwaltungssystemen übernehmen kann.

3.2. Kartenterminal

Kartenterminals werden benötigt, um die unterschiedlichen Smartcards der TI lesen zu können. Diese sind per Internet-Protokoll (IP) mit dem Konnektor verbunden. Dafür werden spezielle Gerätekarten verwendet, die mit den Geräten bereitgestellt werden und die eine gegenseitige sichere Identifikation erlauben. Dafür muss beim ersten Verbinden ein sogenanntes „Pairing“ (Paarbildung) vorgenommen werden, wobei am Kartenterminal eine PIN einzugeben ist, die bestätigt, dass jetzt der physikalisch verwendete Konnektor mit diesem Kartenterminal verbunden werden soll. Muss ein Konnektor ausgetauscht werden, so muss das Pairing wiederholt werden. Um zu vermeiden, dass dabei bei jedem Kartenterminal nochmals eine PIN eingegeben werden muss, kann die Konfiguration eines Konnektors gesichert werden und in einen neuen Konnektor eingespielt werden. Dieser führt dann ein Re-Pairing durch, bei dem er dem Kartenterminal

die alten Pairing-Informationen liefert und damit ein neues Pairing mit der in ihm verbauten Karte veranlasst. Dies soll ohne manuelle Aktivitäten an den Kartenterminals geschehen, ist aber trotzdem mit einem spürbaren Zeitaufwand versehen und stellt aktuell den kritischen Pfad zur Wiederherstellung der Betriebsbereitschaft dar.

Ehemals für die Versichertenkarten vorgesehene Kartenterminals, die als „VSDM-Kartenterminals“ einsetzbar waren, dürfen nicht für medizinische Anwendungen verwendet werden. Im Krankenhaus könnten diese „VSDM-Kartenterminals“ an den administrativen) Aufnahmearbeitsplätzen eingesetzt werden, wenn sichergestellt ist, dass dort nicht auf medizinische Daten zugegriffen wird. Die DKG betont, dass es sinnvoller sein könnte nur eine Geräteart anzuschaffen, egal für welchen Arbeitsplatz, und damit auszuschließen, dass fehlerhafte Verwendungen passieren. Dies können dann nur eHealth-Kartenterminals mit entsprechender Zulassung der gematik sein.

Für jeden Aufnahmearbeitsplatz wird ein Kartenterminal benötigt, das wie beschrieben über eine IP-Verbindung mit dem Konnektor verbunden ist. Dies setzt in der Regel voraus, dass über eine entsprechende Dose und ein IP-Kabel eine Verbindung zu dem entsprechenden Router geschaffen werden muss, wenn vom Kartenterminal keine indirekte Verbindung über einen speziellen USB-Treiber hergestellt wird.

Die Verwendung eines eigenen Virtuellen Local Area Network (VLAN) für Konnektor und die Kartenterminals in Verbindung mit einem Gateway am Übergang zum Primärsystem kann empfehlenswert sein. Abhängig von der Anzahl der eingesetzten Kartenterminals kann es notwendig werden, die IP-Infrastruktur auszubauen und zusätzliche Verteiler (Switches) einzusetzen. Ebenfalls muss beachtet werden, dass eventuell intern verwendete IP-Adressbereiche erweitert werden müssen, wenn z. B. mehr als 254 Geräte einschließlich der Kartenterminals in das interne Netzwerk eingebunden werden müssen.

Neben den Kartenterminals, die mit dem VSDM für das Lesen der eGK bei der Aufnahme bzw. bei der Erfassung ambulanter Patienten verwendet werden, muss für einzelne Anwendungen, z. B. für die Signatur der Notfalldaten, an ärztlichen Arbeitsplätzen ein Kartenterminal verfügbar sein, wenn dort Signaturen mit dem HBA erzeugt werden sollen.

3.3. VPN-Zugangsdienst

Damit der Konnektor sicher mit den Diensten in der TI kommunizieren kann, wird ein spezieller VPN-Zugangsdienst verwendet. Dieser baut einen Virtual-Private Network (VPN)-Kanal, also einen verschlüsselten Tunnel, in die TI auf und wird von zugelassenen Anbietern angeboten. Diese bieten auch einen besonders gesicherten Übergang ins Internet (Secure Internet Service (SIS)) an, der von Arztpraxen oder auch Krankenhäusern genutzt werden kann, wenn vorher kein besonders gesicherter Zugang zum Internet vorgehalten wurde.

Die eigentliche Verbindung in das Internet kann im Prinzip über einen beliebigen Weg geschaffen werden. Die gematik hat die Zulassungs- und Bestätigungsverfahren für VPN-Zugangsdiensteanbieter so gestaltet, dass der eigentliche Betrieb des VPNs von dem Angebot des VPN-Zugangs an Leistungserbringer entkoppelt werden kann. Unterschiedliche Lösungspakete können am Markt angeboten werden.

Da für den Aufbau der Verbindung die Identität des Konnektors geprüft wird, muss für jeden Konnektor ein eigener VPN-Zugangsdienst verwendet werden. Dies führt bei der

Verwendung von mehreren Konnektoren in einem Krankenhaus zu Redundanzen und Mehrkosten, die in der Finanzierungsvereinbarung der DKG mit dem GKV-SV berücksichtigt wurden.

3.4. Institutionskarte (SMC-B)

Zur Nutzung der Dienste der Telematikinfrastruktur (TI) muss sich eine Einrichtung authentisieren. Die Authentisierung stellt dabei den Nachweis dar, dass die Einrichtung tatsächlich diejenige ist, die sie vorgibt zu sein. Hierfür ist eine Security Module Card Typ B-Karte (SMC-B) erforderlich.

Die Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG) ist Herausgeberin für die „SMC-B Krankenhaus“ für stationäre und teilstationäre sowie einige ambulante Organisations- und Leistungsbereiche. Aktuelle Details entnehmen Sie bitte der Webseite der DKTIG (<https://www.dktig.de/de/trustcenter/zustandigkeit-der-dktig>).

Die Möglichkeit zur elektronischen Beantragung einer „SMC-B Krankenhaus“ besteht bereits. Hierbei sollte beachtet werden, dass SMC-B-Karten möglichst 4 bis 6 Wochen vor dem Installationszeitpunkt des Konnektors/der Konnektoren im Krankenhaus über das Antragsportal beantragt werden. Weiterhin sollte beachtet werden, dass die Kartenproduktion erst nach dem Vorliegen sämtlicher Antragsunterlagen bei der DKTIG erfolgt.

Hinweis:

Die kostenpflichtige Zertifikatslaufzeit der SMC-B beginnt mit der Kartenproduktion.

Weitere Informationen zum zeitlichen Ablauf sowie zum Antragsverfahren sind auf der Internetseite der DKTIG abrufbar (<https://www.dktig.de/de/trustcenter/trustcenter-smc-b>).

Die Institutionskarte wird bei jeder Inbetriebnahme einmalig mit einer PIN freigeschaltet und kann dann von allen Berechtigten verwendet werden, ohne dass PIN-Eingaben notwendig werden. Dafür muss allerdings nachvollziehbar elektronisch protokolliert und sichergestellt werden, dass keine unberechtigte Nutzung des SMC-B erfolgt. Dies setzt in der Regel voraus, dass das Primärsystem ein Rollen- und Berechtigungssystem umsetzt, dieses entsprechend gepflegt wird und eine angemessene Protokollierung durchführt. Die Anpassung der bestehenden Systeme an die neuen Anforderungen ist Bestandteil der Finanzierungsvereinbarung. Bei Beantragung der SMC-B wird bestätigt, dass die damit verbundenen Zugriffsrechte gemäß gesetzlicher Vorgaben von einem HBA-Inhaber autorisiert werden. Dies könnte z.B. die medizinische Leitung sein. Der HBA muss dabei nicht in ein Kartenterminal gesteckt werden, die „Inhaberschaft“ des HBA in Verbindung mit der nachprüfbar elektronischen Protokollierung der SMC-B-Zugriffe erfüllt die gesetzlichen Vorgaben.

Eine SMC-B repräsentiert das Krankenhaus bzw. seine Geschäftsführung, und ist auch der Endpunkt für die verschlüsselte Kommunikation mit einem Krankenhaus. Dies bedeutet, dass für jede Rechtseinheit mit Zugriff auf die eGK oder direkter Kommunikation zur TI im Krankenhaus der Einsatz einer eigenen SMC-B sinnvoll sein kann. Insbesondere benötigt in der Regel jedes Medizinische Versorgungszentrum, auch wenn es zum gleichen Träger gehört, eine eigene SMC-B, die über die KV zu beantragen ist.

Es sollte abgewogen werden, für welche Leistungsbereiche eigene SMC-Bs erforderlich sind. Soll z.B. an jedem Standort ein Konnektor stehen, der aus technischen Gründen über eine eigene SMC-B verfügen muss, kann es dazu kommen, dass für eine Organisationseinheit mehrere SMC-B beantragt werden müssen.

Bei der Beantragung ist unbedingt zu beachten, dass mehrere SMC-B für den gleichen Mandanten über die gleiche Telematik-ID verfügen müssen, über die Teilnehmer in der TI technisch identifiziert werden. Gleiches gilt für neue Karten zu einem Mandanten, die mit unveränderter Telematik-ID vor Ablauf einer SMC-B beantragt werden. Davon zu unterscheiden sind SMC-B für bestimmte zusätzliche Bereiche im Krankenhaus, z.B. eine zentrale Poststelle für die Weiterleitung von allgemein an das Krankenhaus adressierten KIM-Nachrichten. Diese Poststelle könnte einen eigenen Mandanten darstellen und müsste dann entsprechend über eine eigene Telematik-ID verfügen, die über die Zeit, auch bei Kartenwechseln, wieder stabil bleiben sollte.

3.5. Heilberufsausweis (HBA)

Ärzte und Gehilfen im Krankenhaus arbeiten in der Regel nach Anmeldung am Krankenhausinformationssystem mit den vorliegenden Daten. Personengebundene Smartcards wie der HBA sind nicht erforderlich, um über den Konnektor auf Daten der eGK oder in der TI zugreifen zu können oder um signierte Daten abzurufen oder zu überprüfen. Einzig für die Erstellung einer qualifizierten elektronischen Signatur (QES) muss ein Heilberufsausweis (HBA) im Krankenhaus in ein Kartenterminal gesteckt werden, wenn die QES für eine Anwendung gesetzlich gefordert ist.

Derzeit wird die QES mit dem HBA für Notfalldaten, den elektronischen Medikationsplan und für eRezepte gefordert, aber auch für Anwendungen, die unabhängig von der TI entwickelt wurden, wie die elektronische Arbeitsunfähigkeitsbescheinigung (eAU). Die Signatur von Daten ist nur dann notwendig, wenn ein Datensatz neu angelegt oder geändert werden soll. Dies wird bei den genannten Anwendungen in der Regel zur Entlassung des Patienten, bzw. wenn er die Ambulanz verlässt, anfallen.

Zu beachten ist, dass die Prozessschritte „Datensatz anlegen/ändern“, „Signatur aufbringen“ und „Datensatz auf eGK schreiben / in ePA einstellen“ nicht direkt hintereinander durchgeführt werden müssen. Angelegte Datensätze können technisch gesehen gesammelt und dann von einem Arzt, der über einen HBA verfügt, mit einer Stapelsignatur „in einem Rutsch“, ohne wiederholte PIN-Eingabe, signiert werden, bevor z.B. Gehilfen das Schreiben auf die eGK bzw. das Einstellen in die ePA übernehmen.

Ob die Stapelsignatur sinnvoll zum Einsatz kommen kann, wird nicht zuletzt davon abhängen, welche Zeit für eine „Stapelbildung“ während der Behandlungsdauer der Patienten bleibt. Je nach Verweildauer unterschiedlicher Patientengruppen (z.B. Chirurgie oder Ambulanz) könnte die QES-Stapelsignatur in Teilbereichen einsetzbar sein. Dann ist auch nur dort die Softwareunterstützung für Stapelsignaturen notwendig.

Neben der Stapelsignatur ist eine Komfortsignatur spezifiziert. Dabei bleibt der HBA nach QES-PIN-Eingabe über den Tag gesteckt und der Arzt kann von unterschiedlichen Arbeitsplätzen einzelne Signaturen komfortabel auslösen, d.h. ohne erneute Eingabe der QES-PIN. Zu beachten ist, dass die unterschiedlichen Arbeitsplätze auf die gleiche Primärsystem-ID beschränkt sind und so die Arbeit in wechselnden Umgebungen eingeschränkt sein kann. Erfahrungen mit Umsetzungen der hier beschriebenen Komfortsignatur im Krankenhaus liegen derzeit noch nicht vor.

Es gibt keine gesetzliche Vorgabe, nach der sich alle Ärzte im Krankenhaus mit einem HBA auszustatten haben. Laborärzte oder Pathologen, die keinen Patientenkontakt haben, können den HBA im Krankenhaus z.B. kaum zum Einsatz bringen. Der HBA ist vielmehr die persönliche Signaturkarte des Arztes mit Ausweis seiner Ärztekammer-Zugehörigkeit und muss vom Arzt selbst beantragt werden. Das Krankenhaus kann den Beantragungsprozess nicht für den Arzt übernehmen. Bei der Überlegung, welche Ärzte einen HBA im Krankenhaus zum Einsatz bringen könnten, spielen insbesondere organisatorische Gegebenheiten die entscheidende Rolle, z.B. welche Ärzte eine dauerhafte Verfügbarkeit von HBA im Entlassmanagement gewährleisten können.

In der Finanzierungsvereinbarung ist eine anteilige Refinanzierung des HBA von den Krankenkassen gegen Nachweis über das Krankenhaus vorgesehen.

3.6. Anpassung Primärsysteme

Zur Nutzung der Telematikinfrasturktur sind Anpassungen an den eingesetzten Primärsystemen erforderlich. Die gematik bietet ein Bestätigungsverfahren an, das die Konformität der Primärsysteme bei der korrekten Ansprache der Konnektor-Schnittstelle bewertet.

Den Leitfaden zur Bestätigung der Konformität des Primärsystems zur Konnektorschnittstelle kann unter <https://fachportal.gematik.de/service/konnektorsimulator-fuer-primarsysteme/bestaetigungsverfahren/> eingesehen werden.

Die Liste der bestätigten Primärsysteme ist unter <https://fachportal.gematik.de/service/konnektorsimulator-fuer-primarsysteme/liste-der-bestaetigten-primarsysteme/> abrufbar.

Neben der Bedienung der Konnektor-Schnittstellen müssen die Krankenhausinformationssysteme die fachlichen Anteile der medizinischen Anwendungen (NFDM, eMP, ePA, usw.) unterstützen. Das Krankenhaus entscheidet, ausgehend von der bestehenden KIS-Installation, welche Anwendungskomponenten in welchen Subsystemen für die Unterstützung der Behandlungsabläufe notwendig sind.

4. Finanzierungsvereinbarung

Zwischen dem GKV-Spitzenverband (Spitzenverband Bund der Krankenkassen) und der Deutschen Krankenhausgesellschaft wurde eine Vereinbarung zur Finanzierung der bei den Krankenhäusern entstehenden Ausstattungs- und Betriebskosten im Rahmen der Einführung und des Betriebs der Telematikinfrastur vereinbart.

Die Vereinbarung regelt auch die Finanzierung der Ausstattung und des Zusatzaufwands der an der Erprobung der Telematikinfrastur (Feldtests) teilnehmenden Krankenhäuser (§ 1).

Regelungsgegenstand ist ferner eine Pauschale für die Erstausrüstung sowie die Kosten im laufenden Betrieb für die Fachanwendungen Notfalldatenmanagement und elektronischer Medikationsplan sowie die sichere Kommunikation im Medizinwesen, ehemals Kommunikation Leistungserbringer (KOM-LE) genannt, bis hin zur ePA.

Die Finanzierungsvereinbarung wird in diesem Jahr fortgeschrieben. Dabei wird z.B. eine Vereinbarung zu der „Beratungspauschale“ bei Erstanlage der ePA für einen Patienten in Höhe von 10 Euro (einmalig je Versichertem abrechenbar) ergänzt werden.

5. Übersicht über die Fristen

Bereiche im Krankenhaus	Anwendungen	Frist zur Anbindung (Sanktion ausgesetzt)	Höhe der Sanktion (% der Rechnung)	Verweis SGB V (Beschlussfassung PDSG) bzw. Hinweise
Ermächtigte und weitere vertragsärztliche Versorgungsbereiche im KH einschließlich Notfallambulanzen nach § 75 Abs. 1b SGB V	VSDM	31.12.2020	2,5 % (ab 1.3.2020)	§ 291b Abs. 5 SGB V
Alle Leistungsbereiche, die NFDM/eMP Lesen oder Schreiben, einschließlich Notfallversorgung nach § 76 Abs. 1 Satz 2 SGB V	NFDM, eMP	keine, gemäß Begründung zum PDSG ab 1.1.2021 vorgesehen	Anrecht des Patienten beachten	VSDM, NFDM und eMP bilden gemäß Finanzierungsvereinbarung die Voraussetzung für den Beginn des „TI-Betriebs“ im KH und für die Vereinbarung des pauschalen Zuschlags in den Budget- und Entgeltverhandlungen
Vertragsärztliche Versorgung	NFDM, eMP	keine, gemäß Begründung zum PDSG ab 1.1.2021 vorgesehen	Patient kann Kopie von NFDM und eMP in ePA verlangen	§ 349 Abs. 3 und 4 SGB V
stationäre Leistungsbereiche einschließlich psychiatrischer und psychosomatischer KH	ePA	31.12.2020	1 % als Abschlag, Klarstellung zur Handhabung in Abstimmung	§ 341 Abs. 7 SGB V
Alle vom Entlassmanagement erfassten Leistungsbereiche, die Onkologie und die KH-Apotheken	eRezept, elektr. Abrechnung	Anbindung Apotheke: 30.9.2020 eRezept: 1.1.2022	keine Anrecht des Patienten beachten	§ 31a Abs. 3 SGB V § 360 Abs. 2 und 3 SGB V i.V.m. § 129a SGB V, § 300 SGB V
Insbesondere vom Entlassmanagement erfasste Leistungsbereiche	eAU	1.1.2021 (ggf. mit Ausnahmen, Rundschreiben beachten)	Recht des Patienten auf Lohnfortzahlung im Krankheitsfall	§ 295 Abs. 1 SGB V in der ab 1.1.2021 gültigen Fassung (TSVG) § 39 Abs. 1a SGB V

5.1. Handhabung Fristen

Der Rollout der Telematikinfrastruktur im niedergelassenen Bereich einschließlich MVZ ist weit fortgeschritten. Die Anbindung der Krankenhäuser an die TI ist nach den oben zusammengestellten Fristen vorgesehen.

Wir gehen davon aus, dass der Rollout der TI wegen Verzögerungen bei der Umsetzung einzelner Anwendungen nicht ausgesetzt wird und Fristen nicht (noch einmal) um ein Jahr verschoben werden. Daraus ergibt sich die Notwendigkeit, die Einführung der Telematikinfrastruktur bzw. der einzelnen Anwendungen im Krankenhaus so vorzubereiten, dass von dem Gesamtkonzept, nach dem alle Anwendungen „gleichzeitig“ eingeführt werden, im Einzelfall abgewichen werden kann.

Das Versichertenstammdatenmanagement ist seit langem spezifiziert und sollte zum 1.1.2021 eingerichtet sein. Gemeinsam mit dem VSDM bilden nach der aktuellen Finanzierungsvereinbarung die Anwendungen eMP und NFDM den „TI-Betriebsbeginn“ und die Grundlage für die Vereinbarung des Telematikzuschlags. Den drei Anwendungen ist gemein, dass sie mit einem PTV3-Konnektor, der in 2020 die Zulassung erlangt hat, umgesetzt werden können. Es bleibt die im Einzelfall zu klärende Frage, wann die Hersteller der jeweils verwendeten Primärsysteme die notwendige Software für die Anwendungen eMP und NFDM bereitstellen.

Eine Besonderheit ist die Anwendung KIM, ein reines Transportmedium für verschlüsselte E-Mails, die eingeführt werden „muss“, um darauf aufbauende Anwendungen wie die eAU umsetzen zu können.

Für die Nutzung der einrichtungsübergreifenden patientengeführten ePA im Krankenhaus stehen bisher weder zugelassene PTV4-Konnektoren noch angepasste Primärsysteme bereit. Insbesondere bei dieser Anwendung werden die Projektverantwortlichen in den Krankenhäusern im Jahresverlauf 2020 prüfen müssen, zu welchem Zeitpunkt die notwendigen Komponenten bereitstehen.

Die Regelungen zu den Anwendungen wie der elektronischen Arbeitsunfähigkeitsbescheinigung oder den Meldeverfahren für Infektionskrankheiten DEMIS, die unabhängig von der TI spezifiziert wurden und auf der TI aufbauen, sowie Änderungen, die sich mit weiteren Gesetzgebungsverfahren nach der Beschlussfassung zum Patientendatenschutz-Gesetz (PDSG) ergeben, werden fortlaufend analysiert und in eigenen Dokumenten aufbereitet. Beachten Sie bitte, wie immer, die Informationen ihrer Krankenhausesellschaft.