Projekt: **EPA.nrw**	
Teilprojekt: **AP 6**	
Gegenstand: **Technische und organisatorische Anforderungen an sichere EPA-Systeme**	
Dokumentname: **Proj_EPA.nrw-AP6_Ausarb-Tech-Org-Anforderungen_V-0-2-4_20070713.doc**	**Version: 0-2-4** **Datum: 13.07.2007** **Uhrzeit: 11:00** **Ersteller: Engels**

Dokumentenhistorie zeitlich absteigend

Version	vom	Kap./Seite	Grund/Hinweis	Durch/Bearbeiter
0-2-4	15.04.2008		Formatierung	Kühn
0-2-3	05.02.2008		Veröffentlichung	Kühn
0-2-2	01.10.2007	Alle	Formatierung	Kühn
0-2-0	30.07.2007		Überarbeitung / Finalisierung	Engels / Kühn
0-1-0	13.07.2007		Initialversion	Engels / Kühn

Verweise zu anderen Dokumenten und Quellen:	**Typ:**
Hinweise zur aktuellen Version: Erstellt durch Jürgen Engels, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen , Düsseldorf	

LDI NRW Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Inhaltsverzeichnis

0 Einleitung und Motivation

Digitale informationstechnische Systeme arbeiten fast ausschließlich mit magnetischen oder elektromagnetischen Zeichendarstellungen. Diese Darstellungen sind für den Menschen ohne technische Hilfsmittel nicht wahrnehmbar. Er kann sie nicht sehen, nicht hören nicht fühlen, nicht riechen, nicht schmecken.

Um zu erkennen, welche Informationen von einem Digitalrechner verarbeit werden, ist der Mensch immer auf Werkzeuge in Form von Hard- und Software angewiesen, welche die magnetischen und elektromagnetischen internen Zeichendarstellungen in für ihn wahrnehmbare externe Repräsentationen umsetzen. Damit gibt es, von Ausnahmen abgesehen, keine Möglichkeit der unmittelbaren Wahrnehmung. Die Vertrauenswürdigkeit der Abläufe und deren Ergebnisse in einem IT-System hängt entscheidend von der Vertrauenswürdigkeit der Hard- und Software ab.

Diese Abhängigkeit hat schwerwiegende Folgen, wenn es sich um rechtsverbindliche Vorgänge handelt, insbesondere auch wenn Informationen verarbeitet werden, auf deren Grundlage Entscheidungen getroffen werden, die für Leib und Leben schwerwiegende Folgen haben können. Aus der Unmöglichkeit der unmittelbaren Wahrnehmbarkeit digitaler Informationen folgt notwendig:

Wo immer moderne Informationstechnik als Werkzeug eingesetzt wird, gibt es keine direkte Inaugenscheinnahme. Damit entfällt für alle Vorgänge die Möglichkeit des Augenscheinbeweises. Der Augenscheinbeweis muss durch andere, völlig neue Techniken ersetzt werden, die mindestens ebenso vertrauenswürdig sein müssen wie die unmittelbare Wahrnehmung.

Daneben sind mit der digitalen Informationsverarbeitung weitere spezifische Probleme verbunden, die aus der analogen Welt nicht bekannt sind. Im Folgenden sind einige dieser besonderen Eigenschaften digitaler Informationen angeführt:

E1: Digitale Informationen können mit den menschlichen Sinnen nicht wahrgenommen werden. Man benötigt hierzu Hard- und Software.

E2: Alle digitalen Informationen werden auf der Ebene der Maschine gleichermaßen binär repräsentiert.

E3: Die externe Darstellung der internen digitalen Information auf der Ebene der Mensch-Maschine-Schnittstelle (in Form von Schrift, Bild oder Ton) beruht auf einer Interpretation der internen, binären Repräsentation.

E4: Digitale Informationen besitzen keine individuellen Merkmale, wie es beispielsweise bei der Handschrift oder der Schreibmaschinenschrift der Fall ist.

E5: Digitalen Informationen ist nicht „anzusehen“, von wem sie stammen.

E6: Digitale Informationen gehen im Allgemeinen keine feste Bindung mit ihrem Trägermedium ein. Deshalb kann man sie leicht verändern oder löschen, ohne Spuren zu hinterlassen.

E7: Digitale Informationen sind sehr verletzlich, z.B. durch magnetische oder elektromagnetische Einflüsse. Schon kleine Verletzungen können gravierende Folgen haben. Wird nur ein Bit des Schlüssels verschlüsselter Daten verändert, ist die Information nicht mehr entschlüsselbar.

E8: Digitale Informationen können leicht und unbemerkt übertragen werden, sogar weltweit via Internet.

E9: Eine Übertragung digitaler Informationen bedeutet die Erzeugung vielfacher Kopien. Bei einer Datenübertragung via Internet ist nicht nachvollziehbar auf welchen Systemen sich die Kopien befinden und wie lange sie dort gespeichert bleiben.

E10: Digitale Informationen sind nicht dauerhaft, da einerseits ihre Trägermedien relativ schnell altern und andererseits zur Interpretation der Informationen die entsprechende Software vorhanden sein muss, die selbst wiederum eine digitale Information darstellt. Darüber hinaus ist die Hardware erforderlich, auf der die Interpretationssoftware lauffähig ist.

Aus diesen besonderen Eigenschaften der digitalen Informationsverarbeitung resultieren Probleme, die – wenn überhaupt – nur mit einem hohen technischen Aufwand zu bewältigen sind:

P1: Aus den Eigenschaften E1 bis E3 ergibt sich das Problem der **Informationsvalidität**:

Wie kann man sicher sein, dass die dargestellte Information der wirklichen Information entspricht?

P2: Aus den Eigenschaften E4 und E5 ergibt sich das **Urheberschaftsproblem**:

Wie weiß man sicher, aus welcher Quelle eine Information stammt?

P3: Aus den Eigenschaften E6 und E7 folgt das **Integritätsproblem**:

Wie kann man sicher sein, dass eine Information nicht verändert wurde?

P4: Aus den Eigenschaften E8 und E9 ergibt sich das **Vertraulichkeitsproblem**:

Wie kann man sicherstellen, dass eine Information nicht Unbefugten zur Kenntnis gelangt?

P5: Aus E10 ergibt sich das **Persistenzproblem**:

Wie kann man sicherstellen, dass eine Information auch noch über einen langen Zeitraum vorhanden und verfügbar ist?

Insbesondere für die einem hohen bis sehr hohen Schutzbedarf unterliegenden EPA-Systeme müssen Lösungen gefunden werden, welche die mit den besonderen Eigenschaften digitaler Informationssysteme verbundenen spezifischen Probleme, die in der analogen Welt nicht bekannt sind, in angemessener Weise berücksichtigen und beherrschbar machen.

1 Kriterien für sichere EPA-Systeme

Ziel muss die Entwicklung sicherer EPA-Systeme sein. Dieses Ziel ist nur erreichbar, wenn EPA-Systeme aus zwei Sichten heraus als sicher betrachtet werden können:

sichere EPA-Systeme müssen verlässlich sein

sichere EPA-Systeme dürfen ihre Benutzer und die Betroffenen nicht beeinträchtigen, weder direkt noch indirekt, d.h. sie müssen beherrschbar sein.

Für das Werkzeug EPA-System folgen daraus zwei Anforderungen an die Sicherheit, die als zwei einander ergänzende, zueinander komplementäre Sichten den vollständigen Bedeutungsinhalt von Sicherheit beschreiben:

EPA-Systeme können nur als sicher betrachtet werden, wenn sie sowohl **verlässlich** als auch **beherrschbar** sind.

Nur unter dieser dualen Sichtweise sind sichere EPA-Systeme realisierbar. Jede Sicht wird definiert durch Sicherheitsziele, die in der folgenden Tabelle zusammengestellt sind.

Sicherheit	
Verlässlichkeit - Sicherheit des Systems -	Beherrschbarkeit - Sicherheit vor dem System -
Vertraulichkeit Integrität Verfügbarkeit	Zurechenbarkeit Nutzungsfestlegung Informationsqualität und -validität Revisionsfähigkeit Nicht-Abstreitbarkeit der Kommunikation Rechtsverbindlichkeit Betroffenenrechtsgarantie Alltagstauglichkeit Barrierefreiheit

Die Umsetzung dieser Sicherheitsziele in spezifische technische und organisatorische Maßnahmen für ein EPA-System, erfordert die Erstellung eines individuellen Sicherheitskonzepts auf der Grundlage einer Schutzbedarfsermittlung sowie einer Bedrohungs- und Risikoanalyse. Eine detaillierte Sicherheitsanalyse setzt ein konkretes System voraus und kann deshalb erst dann durchgeführt werden, wenn die Architektur, die Technologie, die Funktionalität etc. feststehen. Von einem gewissen Abstraktionsniveau aus betrachtet haben EPA-Systeme allerdings Gemeinsamkeiten, für die grundlegende Anforderungen an die Technik und die Organisation definiert werden können, ohne das reale System zu kennen. Im folgenden Kapitel werden für die einzelnen Sicherheitsziele solche essentiellen Anforderungen beschrieben. Diese Kernanforderungen muss jedes EPA-System erfüllen, unabhängig von seiner konkreten Ausprägung. Die Anforderungen werden dabei bewusst und so weit eben möglich technikneutral formuliert, um unterschiedliche Implementierung zu ermöglichen und bestimmte

Technologien nicht von vorn herein auszuschließen. Weitergehende Sicherheitsanalysen sind dann jeweils für ein konkretes EPA-System nach der Methodik des Bundesamtes für Sicherheit in der Informationstechnik, individuell und im Detail anzustellen.

2 Grundlegende technische und organisatorische Anforderungen zur Gewährleistung der Sicherheitskriterien

2.1 Gewährleistung der Vertraulichkeit

2.1.1 Definition Vertraulichkeit

Die Vertraulichkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. eine unbefugte Kenntnisnahme von Daten oder ein unbefugtes Erschließen von Informationen muss in jeder Verarbeitungsphase ausgeschlossen werden.

„Wer sich in Behandlung begibt, muss und darf erwarten, dass alles, was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim bleibt und nicht zur Kenntnis Unberufener gelangt. Nur so kann zwischen Patient und Arzt jenes Vertrauen entstehen, das zu den Grundvoraussetzungen ärztlichen Wirkens zählt, weil es die Chancen der Heilung vergrößert und damit - im ganzen gesehen - der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient (BVerfG 32, 373, 380).“

Die in den ärztlichen Berufsordnungen (§ 9 M-BO) und dem Strafgesetzbuch (§ 203 StGB Abs. 1 Nr. 1) normierte ärztliche Schweigepflicht schützt das Verhältnis zwischen Patient und Arzt. Der Arzt muss die Vertraulichkeit der erhobenen, gespeicherten, übermittelten und sonst verarbeiteten Daten gewährleisten. Nicht zu übersehen ist, dass eine unbefugte Offenbarung auch durch Unterlassen verwirklicht werden kann, zum Beispiel dadurch, dass der zur Verschwiegenheit Verpflichtete nicht verhindert, dass sich ein Dritter Kenntnis von den anvertrauten Informationen verschafft. Vor diesem Hintergrund kann die Nutzung eines EPA-Systems, dass Patientendaten mit fehlendem, beziehungsweise mangelndem Vertraulichkeitsschutz verarbeitet, so dass unbefugte Dritte potentiell in der Lage wären, auf die zu schützenden Daten zuzugreifen, bereits strafrechtlich relevant werden.

Auch die datenschutzrechtlichen Regelungen, die das Recht des Patienten auf informationelle Selbstbestimmung konkretisieren, schützen das Vertrauensverhältnis zwischen Arzt und Patient in besonderem Maße. Gesundheitsdaten gehören zu den Daten, die als besondere Arten von personenbezogenen Daten, einem besonderen Schutz unterliegen (§ 3 Abs. 9 BDSG).

Starke Mechanismen zur Gewährleistung der Vertraulichkeit sind damit essentiell für ein sicheres EPA-System. Kann die Vertraulichkeit während aller Verarbeitungsphasen nicht wirksam sichergestellt werden, ist Ärzten die Nutzung eines solchen Systems nicht zuzumuten, da sie letztlich verantwortlich sind für die Gewährleistung der Vertraulichkeit, der im Rahmen ihrer Berufsausübung gewonnenen Patientendaten und ihre Verantwortlichkeit auch nicht abgeben können. Oder anders ausgedrückt: Die Nutzung eines EPA-Systems ohne hinreichenden Vertraulichkeitsschutz, kann dazu führen, dass sich die nutzenden Ärzte dem Vorwurf einer unbefugten Offenbarung geheim zu haltender Daten ausgesetzt sehen müssen.

„Zu beachten ist ferner, dass elektronisch gespeicherte medizinische Daten nicht nur für medizinische Fachkräfte von Interesse sind, sondern auch das Interesse von Dritten, wie etwa Versicherungsunternehmen oder Strafverfolgungsbehörden wecken können. Aus Sicht des Datenschutzes bergen EPA-Systeme, welche die medizinischen Daten einer Person aus verschiedenen Quellen zentral erfassen und diese sensiblen Daten weiteren Kreisen leichter zugänglich machen, ein neues Risikopotential, das die Dimensionen des möglichen Missbrauchs medizinischer Daten einzelner Personen völlig verändert [Art29DG].“

In letzter Konsequenz kann eine unbefugte Kenntnisnahme medizinischer Daten (z.B. durch Arbeitgeber, Versicherungen, Pharmaindustrie, Provider) für die Patienten erhebliche soziale oder materielle Folgen nach sich ziehen und für die Ärzte berufsrechtliche (z.B. Entzug der Approbation), haftungsrechtliche (z.B. Schadenersatz auch für Nichtvermögensschäden) und strafrechtliche (z.B. Geldstrafe, Freiheitsstrafe, Berufsverbot) Sanktionen bedeuten.

Daher bilden Mechanismen zur Sicherstellung der Vertraulichkeit die Basis eines von allen Beteiligten als vertrauenswürdig akzeptierbaren EPA-Systems.

2.1.2 Grundlegende Anforderungen zur Vertraulichkeitsgewährleistung

2.1.2.1 Medizinische Daten der Patienten

Informationsobjekt	**medizinisches Datenobjekt (MDO)** Die MDOs repräsentieren die medizinischen Inhaltsdaten einer EPA. Ein MDO ist atomar, d.h. aus medizinisch-fachlicher Sicht in sich abgeschlossen und nicht weiter zerlegbar.
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18-So019)
Kernanforderungen	
Vertr-MDO-01	Die MDOs liegen durchgängig Ende-zu-Ende (Person-zu-Person) nur in verschlüsselter Form vor. Das heißt die Verschlüsselung eines MDO erfolgt vor dem Upload in die EPA und die Entschlüsselung erfolgt nach dem Download aus der EPA, jeweils in den beteiligten Primärsystemen. Die MDOs sind damit auf dem EPA-Server verschlüsselt.
Vertr-MDO-02	Die zur Anwendung kommenden kryptographischen Verfahren müssen die ungerichtete Kommunikation unterstützen. Die ungerichtete Kommunikation ist in einem EPA-System als Regelfall anzusehen, da zum Zeitpunkt des Einstellens eines MDO in eine EPA der Nutzer des MDO grundsätzlich noch nicht feststeht. Patienten haben das Recht auf freie Arzt- und Krankenhauswahl und außerdem sind EPA-Systeme gerade als Systeme zur asynchronen, zeitversetzten Kommunikation konzipiert, da in eine EPA MDOs eingestellt werden, deren Nutzung erst in späteren, noch nicht notwendigerweise bekannten Behandlungssituationen erfolgen wird.
Vertr-MDO-03	Das kryptographische Verfahren muss gewährleisten, dass die Ver- und Entschlüsselung eines MDO nur möglich ist unter Verwendung eines individuellen Geheimnisses des Patienten, das in dessen Verfügungsgewalt

		ist. Durch diesen Mechanismus wird eine Autorisierung durch den Patienten in einem konkreten Behandlungskontext erzwungen.
	Vertr-MDO-04	Das technische Verfahren muss gewährleisten, dass auch ein Vertreter des Patienten die kontextabhängige Autorisierung für diesen vornehmen kann. Da aufgrund der im Gesundheitswesen möglichen Behandlungssituationen, Konstellationen eintreten können, die eine a priori Vertreterbestimmung ausschließen, muss das Verfahren auch eine ad hoc Vertreterlösung ermöglichen. Der Vertreter muss dann in der Lage sein die kontextabhängige Autorisierung für den vertretenen Patienten durchzuführen und zwar mit den gleichen Möglichkeiten die auch der Vertretene hätte, wenn er selbst agieren könnte. Als Vertreter müssen auch Personen handeln können, die nicht explizit schriftlich vom Patienten dazu bestimmt werden oder wurden, sondern in der konkreten Situation entsprechend den in der analogen Welt akzeptierten Regeln als solche angenommen werden können (z.B. Familienangehörige).
	Vertr-MDO-05	Das Verfahren muss sich in die fachlichen und organisatorischen Abläufe und Gegebenheiten der medizinischen Einrichtungen integrieren. Dabei sind insbesondere folgende Aspekte zu berücksichtigen: 1. MDOs (z.B. Anamnese, Befunde, Diagnosen) werden häufig erst erstellt und in die EPA eingestellt, wenn der Patient die medizinische Einrichtung bereits verlassen hat. Damit muss das kryptographische Verfahren eine Verschlüsselung eines MDO ermöglichen ohne, Mitwirkung des Patienten zum Verschlüsselungszeitpunkt. Dennoch sollte ein Einstellen eines MDO in die EPA nur mit expliziter Autorisierung möglich sein. Das heißt die Autorisierung muss zeitlich vor der Verschlüsselung erfolgen können und der Verschlüsselungsvorgang selbst muss ohne direkte Mitwirkung des Patienten möglich sein. 2. Die MDOs einer EPA werden nicht notwendigerweise beim ersten Patientenkontakt gelesen, sondern häufig erst dann, wenn kein unmittelbarer Patientenkontakt mehr besteht. Damit muss das Verfahren zur Autorisierung im Behandlungskontext es ermöglichen, das die MDO-Entschlüsselung zeitlich nach der Autorisierung durch den Patienten erfolgen kann und keiner Patientenmitwirkung zum Entschlüsselungszeitpunkt bedarf. 3. In Krankenhäusern - im Gegensatz zu Arztpraxen - befinden sich die IT-Systeme in Räumen, zu denen Patienten keinen Zugang haben. Damit muss das Verfahren der expliziten Autorisierung durch den Patienten es ermöglichen, dass die zur MDO Ver- und Entschlüsselung erforderliche Verwendung des individuellen Geheimnisses auch bei einer räumlichen Entfernung der Patienten zur KIS-Umgebung erfolgen kann.
	Vertr-MDO-06	Das Verfahren muss die Erfordernisse und Gegebenheiten in der Patientenversorgung entsprechend unterstützen und darf die bestehenden flexiblen Möglichkeiten der analogen Datenverarbeitung nicht einschränken. Dabei sind u.a. folgende Situationen zu berücksichtigen: 1. Heute haben Patienten die Möglichkeit ihren Arzt telefonisch zu konsultieren. Das kryptographische Autorisierungsverfahren sollte dies ebenfalls

	unterstützen. Beispiel: Ein Patient wird aus dem Krankenhaus entlassen, ist aber zu Hause weiterhin auf das Bett angewiesen. Der Entlassbericht wird für den Hausarzt in die EPA des Patienten eingestellt. Es sollte nun möglich sein, dass der Patient den Hausarzt telefonisch zur Entschlüsselung autorisieren kann, indem er ihm das Autorisierungsgeheimnis zur Entschlüsselung fernmündlich übermittelt. Das bedeutet, die Autorisierung durch den Patienten sollte auch ohne seine persönliche Anwesenheit in der medizinischen Einrichtung möglich sein. 2. Bei Hausbesuchen hat der Arzt keinen Zugriff auf sein Praxisverwaltungssystem. Zur Vorbereitung des Hausbesuchs muss es ihm möglich sein, die relevanten Informationen der EPA des Patienten zu sichten. Hierzu ist es erforderlich, dass er die entsprechenden MDOs entschlüsseln kann, ohne eine Mitwirkung des Patienten, die dessen körperliche Anwesenheit erfordert. formationen zu verschlüsseln und in die EPA einzustellen. Der Mechanismus zur expliziten Autorisierung sollte auch diese Situationen unterstützen können.
Vertr-MDO-07	Das Verfahren muss für die Patienten barrierefrei sein. Dies betrifft insbesondere den Aspekt der expliziten Autorisierung durch den Patienten im Behandlungskontext, also den Mechanismus, der die Ver- und Entschlüsselung seiner MDOs ermöglicht. Das „Übergabeverfahren“ des persönlichen Geheimnisses durch den Patienten muss deshalb technisch und organisatorisch so ausgestaltet sein, dass auch ältere Patienten, Ausländer, Patienten mit einer geistigen oder körperlichen Einschränkung etc. in akzeptabler Art und Weise (entsprechend den Anforderungen, die auch analoge Abläufe an sie stellen) damit umgehen können. Das Gesundheitswesen zeichnet sich eben dadurch aus, dass es mit allen Bevölkerungsgruppen in Kontakt kommt und natürlich eben mit Patienten, also Menschen, die aufgrund ihres Gesundheitszustandes in der Ausübung ihrer Rechte eingeschränkt sind.
Vertr-MDO-08	Die zu wählenden kryptographischen Algorithmen und deren Mechanismenstärke richten sich nach den Richtlinien des BSI.
Vertr-MDO-09	Es muss ein sicheres Key Recovery bzw. Key Escrow Konzept existieren, für den Fall, dass das kryptographische Schlüsselmaterial (Autorisierungsgeheimnis) eines Patienten nicht mehr verfügbar ist oder kompromittiert wurde. Das Verfahren muss sicherstellen, dass die Schlüsselwiederherstellung bzw. die Schlüsselhinterlegung auf einem speziellen Geheimnis basiert, dass nur dem Patienten bekannt ist und sich in dessen Verfügungsgewalt befindet.
Vertr-MDO-10	Das kryptographische Verfahren muss hinreichend flexibel sein, so dass die Längen der kryptographischen Schlüssel entsprechend den sich ergebenden, zukünftigen Sicherheitsanforderungen angepasst werden können und sogar ein Umstieg auf andere kryptographische Algorithmen möglich ist.
Bemerkung	Kyptographische Verfahren beinhalten ein nicht zu vernachlässigendes Risikopotential: 1. Die Sicherheit von symmetrischen Verfahren ist mathematisch nicht be-

	weisbar. Deshalb ist immer damit zu rechnen (wie in der Vergangenheit bereits geschehen), dass eine Schwachstelle eines Verfahrens aufgedeckt wird und damit diemit diesem Verfahren verschlüsselten Daten keinen hinreichenden Vertraulichkeitsschutz mehr haben. 2. Asymmetrische Verfahren basieren auf mathematischen Problemstellungen, für die keine effiziente Lösung bekannt ist. Es ist aber nicht beweisbar, dass ein effizientes Lösungsverfahren nicht existiert. Grundsätzlich muss man also damit rechnen, dass ein effizienter Algorithmus gefunden wird. In einem solchen Fall könnten die mit diesem Verfahren verschlüsselten Daten in angemessener Zeit von einem Angreifer entschlüsselt werden. 3. Unabhängig von den grundsätzlichen Aspekten kryptographischer Verfahren besteht ein Zusammenhang zwischen der Länge der verwendeten Schlüssel und der Leistungsfähigkeit von Prozessorsystemen. Die Schlüssellängen müssen daher ständig an die Zunahme der Rechenkapazität der Computersysteme angepasst werden. Das bedeutet aber, dass Daten, die mit zwischenzeitlich überholten Schlüssellängen verschlüsselt wurden, nicht mehr hinreichend sicher sind. 4. Mit der Verfügbarkeit von Quantencomputern dürften alle bisherigen kryptographischen Verfahren obsolet oder zumindest stark bedroht sein. In diesem Fall wäre man gezwungen auf die Quantenkryptographie zu wechseln. Dies würde eine völlige Neuorientierung bedeuten. Die Auswirkungen sind jetzt noch nicht abschätzbar.
Konsequenzen:	
•	Es ist frühzeitig eine Strategie und ein Notfallkonzept zu entwickeln, wie bei Kompromittierung eines kryptographischen Verfahrens vorzugehen ist. • Es ist festzulegen, wie bei einer erforderlich werdenden Schlüssellängenanpassung vorzugehen ist. • Es ist gut zu überlegen, ob als asymmetrisches Verfahren RSA noch gewählt werden sollte oder unter Aspekten der Zukunftssicherheit ECC der Vorzug zu geben ist. • Elektronische Patientenakten, die über einen langen Zeitraum Bestand haben sollen, sind als sehr kritisch anzusehen. • Die Übermittlung von MDOs via Internet ist aufgrund der nicht kontrollierbaren Zwischenspeicherung auf Vermittlungsrechnern sehr problematisch.
Folgerung	Es ist ein umfassendes Konzept für ein sicheres, praxistaugliches und barrierefreies kryptographisches Verfahren zu entwickeln. Dabei sind insbesondere die Geschäftsvorfälle des Gesundheitswesens zu berücksichtigen. Ein Kryptographieverfahren, dass zwar unter Sicherheitsaspekten geeignet ist, aber sich nicht entsprechend in die organisatorischen und fachlichen Abläufe einfügt, ist für die Praxis nicht geeignet und kann selbst wiederum zum Sicherheitsrisiko werden. Da die Sicherstellung der Vertraulichkeit eine Kernanforderung für ein akzeptables EPA-System ist, kommt dem Kryp-

	tographiekonzept eine besondere Bedeutung zu. Hierbei sollte man besonders sorgfältig vorgehen und keine frühzeitigen Entscheidungen für eine bestimmte Technologie treffen. Zunächst sind die Abläufe und Anforderungen des Gesundheitswesens in Bezug auf ein EPA-System detailliert zu untersuchen. Dann erst ist zu entscheiden, welche Technologie hierfür die beste Unterstützung bietet. Es könnte sich sogar herausstellen, dass unter Berücksichtigung aller Anforderungen, mit der heute zur Verfügung stehenden Technik, kein hinreichender Vertraulichkeitsschutz gewährleistet werden kann bzw. keine adäquate Prozessintegration möglich ist.

2.1.2.2 Metadaten zu den medizinischen Daten

Informationsobjekt	**Metadaten zu medizinischen Datenobjekten (MDO_Meta)** Ein Metadatum beschreibt ein Informationsobjekt MDO. Da die MDOs alle verschlüsselt sind, dienen die Metainformationen den berechtigten Nutzern zur Vorselektion. Greift ein Nutzer lesend auf eine EPA zu, werden ihm die Metadaten derjenigen MDOs angezeigt, für die er eine Leseberechtigung hat. Aufgrund der Metainformationen kann er dann die MDOs selektieren, die für ihn relevant sind und deren Inhalt er zur Kenntnis nehmen möchte.
Schutzbedarfsstufe	**hoch** Begründung: • Können die Metadaten einer konkreten Person zugeordnet werden, so ist bekannt, dass sie sich in ärztlicher Behandlung befindet oder befand. Da Metadaten der Beschreibung der MDO-Inhalte dienen, sind darüber hinaus Rückschlüsse auf Erkrankungen der Person möglich. Dies wäre eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts dieser Person. • Ein möglicher Missbrauch der Kenntnis von bestimmten Erkrankungen einer Person kann erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse dieser Person haben. • Wird bekannt, dass ein EPA-System Rückschlüsse auf die Erkrankungen der EPA-Inhaber ermöglicht, ist mit einer breiten Ansehens- und Vertrauensbeeinträchtigung des Betreibers des EPA-Systems zu rechnen.
Kernanforderungen	
Vertr-MDO_Meta-01	Die Meta-Daten sind bei Übermittlungen durchgängig Ende-zu-Ende vom Quellsystem zum Zielsystem auf Anwendungsebene (gemeint ist die Anwendungsebene des OSI-Modells) zu verschlüsseln. Die Metadaten liegen damit auf dem EPA-System im Klartext vor.
Vertr-MDO_Meta-02	Die Meta-Daten zu den MDOs sind zu pseudonymisieren, d.h. sie sind in ihrem Informationsgehalt so rudimentär zu halten, dass ein Rückschluss auf den EPA-Inhaber nicht möglich ist. Dies ist nur realisierbar, wenn die Metadaten keine Freitexte zulassen, sondern den Benutzern nur eine fest vorgegebene Datenauswahl zur Verfügung steht.
Vertr-MDO_Meta-03	Sollte Anforderung Vertr-MDO_Meta-02 nicht erfüllbar sein, z.B. weil die Aussagekraft der Metadaten durch diese Anforderung zu gering wird, muss

	eine Lösung implementiert werden, die es ermöglicht, dass die Metadaten auch auf dem EPA-System in verschlüsselter Form vorliegen.
Eine solche Lösung könnte beispielsweise wie folgt aussehen:	
	Die Metadaten werden im Quellsystem asymmetrisch mit dem öffentlichen Schlüssel des EPA-Systems verschlüsselt. Greift nun ein Nutzer lesend auf das EPA-System zu, werden alle Metadaten, für deren MDOs er eine Leseberechtigung hat, selektiert und anschließend umgeschlüsselt. Dazu werden die Daten zunächst mit dem geheimen Schlüssel des EPA-Systems entschlüsselt und anschließend für eine Ende-zu-Ende Kryptographie für das aufrufende Primärsystem verschlüsselt. Der Prozess der Umschlüsselung muss dabei in einer gesicherten Umgebung (z.B. Kryptobox) erfolgen.

2.1.2.3 Identifikator der elektronischen Patientenakte

Informationsobjekt	**EPA-Identifikator (EPA_ID)** Der EPA-Identifikator dient der Referenzierung der zu einem Patienten gehörenden elektronischen Patientenakte in ihrer Gesamtheit. Jede EPA-ID ist eindeutig einem Patienten zugeordnet.
Schutzbearfsstufe	**hoch** Begründung: • Wird eine EPA-ID kompromittiert, ist wegen der eindeutigen Zuordnung bekannt, dass eine bestimmte Person im Besitz einer elektronischen Patientenakte ist. Damit kann man davon ausgehen, dass sie sich in ärztlicher Behandlung befindet oder befand. Abhängig von der Person, um die es sich handelt, kann diese Information erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse dieser Person haben. • Wird bekannt, dass eine EPA-ID eines EPA-Systems kompromittiert wurde, ist für den Betreiber des EPA-Systems eine breite Ansehens- und Vertrauensbeeinträchtigung zu erwarten. • Allein die Tatsache, dass sich eine Person in ärztlicher Behandlung befindet, ist eine Information, die unter die ärztliche Schweigepflicht fällt (zuletzt OLG Karlsruhe). Bei Kompromittierung einer EPA-ID könnten Ärzte sich dem Vorwurf der Schweigepflichtverletzung ausgesetzt sehen (möglicherweise durch Unterlassung).
Kernanforderungen	
Vertr-EPA_ID-01	Die EPA-ID muss als Pseudonym implementiert werden. Das heißt, ausgehend von der EPA-ID ist keine Personenzuordnung möglich. Eine Zuordnung ist nur ausgehend von der Person zur EPA-ID möglich. Der Zuordnungsmechanismus ist damit als Einbahnstrasse zu realisieren.
Vertr-EPA_ID-02	Das als EPA-ID verwendete Pseudonym ist rein anwendungsbezogen. In anderen Anwendungszusammenhängen darf es nicht verwendet werden. Hat eine Person mehrere EPAs, sind jeweils unterschiedliche Pseudonyme zu vergeben.

Vertr-EPA_ID-03	Das Pseudonym wird systemintern auf eine OID abgebildet. In der Kommunikation mit anderen Systemen wird nur diese OID verwendet. Innerhalb des EPA-Systems ist die Zuordnungstabelle Pseudonym □ OID in einem von den elektronischen Patientenakten getrennten und besonders gesicherte Systembereich zu halten.
Hinweis	Folgende Lösungsmöglichkeiten sind denkbar: 1. Der Patient erhält die ID seiner EPA in seine Verfügungsgewalt. Eine Referenzierung seiner EPA ist dann nur möglich, wenn er dem Zugreifenden die ID mitteilt bzw. aushändigt. 2. Daten, die den Patienten eindeutig identifizieren, werden durch einen vertrauenswürdigen Pseudonymisierungsdienst verschlüsselt. Das so entstehende Kryptogramm bildet die EPA-ID. Ein Zugriff auf eine EPA müsste dann immer über den Pseudonymisierungsdienst erfolgen. Es ist natürlich sicherzustellen, dass die Nutzung des Pseudonymisierungsdienstes nur für Berechtigte möglich ist. Bei dieser Lösungsvariante ist es allerdings möglich, dass ein berechtigter Nutzer des Pseudonymisierungsdienstes Probezugriffe durchführen kann. Anmerkung: • Die üblicherweise für solche Problemfälle verwendeten kryptographischen Hashfunktionen sind keine gute Lösung. Einerseits sind Kollisionen denkbar (von Praktikern meist unterschätzt), andererseits eröffnen sich bei dieser Vorgehensweise Möglichkeiten für Wörterbuchangriffe. • Auf den ersten Blick könnte eine weitere Lösungsvariante darin bestehen, dass Daten, die den Patienten eindeutig identifizieren, mit einem kryptographischen Schlüssel des Patienten verschlüsselt werden. Das Kryptogramm wäre dann die EPA-ID. Hierbei ist zu bedenken, dass kryptographische Verfahren nicht gewährleisten, dass verschiedene Daten, die mit verschiedenen Schlüsseln verschlüsselt werden, auch zu verschiedenen Kryptogrammen führen. Mit anderen Worten, es kann der Fall eintreten, dass für verschiedene Patienten, die zudem verschiedene Schlüssel nutzen, dieselbe EPA-ID erzeugt wird.
Bemerkung	• Ein Master Patient Index, der sich unter technischen Gesichtspunkten zur Aktenreferenzierung anbieten würde, ist sowohl datenschutzrechtlich als auch verfassungsrechtlich unzulässig. • Die Verwendung der neuen, eindeutigen Krankenversichertennummer im Klartext ist ebenso unzulässig, da sie eine Person eindeutig identifiziert.
Folgerung	Es ist ein Pseudonymisierungskonzept zu entwickeln. Dabei ist zu berücksichtigen, dass das Verfahren - entsprechend den Anforderungen an das Kryptographieverfahren - alltagstauglich, praktikabel und barrierefrei ist. Anzustreben ist ein schlüssiges Gesamtkonzept für ein integriertes Kryptographie- und Pseudonymisierungsverfahren.

2.1.2.4 Personenbezogene Daten der das EPA-System nutzenden Heilberufler

Informationsobjekt	**Personenbezogene Daten der Heilberufler (HB_Data)** Da ein EPA-System alle Verarbeitungsvorgänge zu Revisionszwecken und zur Gewährleistung des Auskunftsrechts der Patienten personenscharf protokollieren muss, enthalten die Protokolldateien identifizierende Daten von Heilberuflern. Darüber hinaus dient eine Protokollierung der Aufzeichnung sicherheitsrelevanter Ereignisse, mit dem Ziel der Verhinderung bzw. der Verfolgung von missbräuchlichen Zugriffen bzw. Zugriffsversuchen.
Schutzbedarfsstufe	**hoch** Begründung: • Die Protokolldaten erlauben prinzipiell die Erstellung von Nutzer- und Nutzungsprofilen. Eine Profilerstellung wäre eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts der betroffenen Heilberufler. Außerdem könnte ein Missbrauch der Protokollinformationen erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der betroffenen Heilberufler haben. • Ein möglicher Missbrauch der Protokollinformationen würde seitens der Heilberufler zu einem breiten Vertrauensverlust in die Nutzung von EPA-Systemen führen, verbunden mit einem Ansehensverlust des EPA-Betreibers, der als Folge mit beachtlichen finanziellen Verlusten rechnen muss.
Kernanforderungen	
Vertr-HB_Data-01	Die Protokollierung zur Gewährleistung der Revisionsfähigkeit und des Auskunftsrecht der Betroffenen ist von der Protokollierung zur Gewährleistung der Systemsicherheit zu trennen.
Vertr-HB_Data-02	In den Protokolldateien dürfen nur pseudonymisierte Daten der Heilberufler erfasst werden.
Vertr-HB_Data-03	Die Anmeldung eines Nutzers am EPA-System erfolgt bereits unter dessen Pseudonym. D.h. eine Pseudonymisierung der identifizierenden Daten der Heilberufler findet zeitlich vor einem EPA-Zugriff und getrennt auf einem anderen System statt, das nicht der Kontrolle des EPA-Betreibers unterliegt.
Vertr-HB_Data-04	Die Zuordnung eines Pseudonyms zu den zugehörigen identifizierenden Daten eines Heilberuflers darf nur durch eine vertrauenswürdige Stelle möglich sein. Diese Stelle ist organisatorisch von der Stelle, die das EPA-System betreibt, zu trennen.
Vertr-HB_Data-05	In Fällen, in denen eine Protokollauswertung erforderlich wird und zulässig ist, führt die vertrauenswürdige Stelle die Depseudonymisierung durch.
Vertr-HB_Data-06	Das Verfahren der Pseudonymisierung ist in einem Pseudonymisierungskonzept festzulegen und muss entsprechend dem Schutzbedarf, hohe Sicherheitsmechanismen aufweisen.
Vertr-HB_Data-07	Welche Stelle für die Pseudonymerzeugung und Depseudonymisierung verantwortlich ist und wie die jeweiligen Verfahrensabläufe erfolgen sollen, ist in einem Organisationskonzept festzulegen. Dabei sind geeignete Verfahren zur Protokollauswertung unter dem Aspekt Revision und Auskunft

	sowie zur schnellen Ermittlung bzw. Verfolgung von Missbräuchen bzw. Missbrauchsversuchen festzulegen.
Hinweis	Ein Pseudonymisierungverfahren könnte beispielweise wie folgt aussehen: Ein Nutzer, der auf eine EPA zugreifen möchte, authentifiziert sich zunächst gegenüber einem vertrauenswürdigen Authentifizierungsdienst. Der Authentifizierungsdienst stellt ein Zertifikat für den Zugriff auf die EPA aus. Das Zertifikat enthält (neben anderen Angaben) das vom Authentifizierungsdienst für diesen Nutzer vergebene Pseudonym.
Anmerkung	Auf den ersten Blick würde sich auch folgendes, auf asymmetrischer Verschlüsselung basierendes Verfahren anbieten: Die identifizierenden Daten der Nutzer werden in den Primärsystemen mit dem öffentlichen Schlüssel einer vertrauenswürdigen Stelle verschlüsselt. Das resultierende Kryptogramm ist das Pseudonym des jeweiligen Nutzers. Eine Entschlüsselung des Pseudonyms wäre dann nur mit dem geheimen Schlüssel der vertrauenswürdigen Stelle möglich. Problem: Ein solches Verfahren ist angreifbar, indem der Angreifer mit dem öffentlichen Schlüssel, identifizierende Daten der Nutzer probeverschlüsselt und die entstehenden Kryptogramme mit den Pseudonymen der Protokolldateien vergleicht (vorausgesetzt er hat darauf Zugriff, was für Betreiber des EPA-System gegeben ist).

2.2 Gewährleistung der Integrität

2.2.1 Definition Integrität

Die Integrität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet werden, d.h. personenbezogene Daten müssen während aller Phasen der Verarbeitung unversehrt, vollständig, gültig und widerspruchsfrei bleiben.

Der Behandlungsauftrag in Einrichtungen des Gesundheitswesens umfasst eine sorgfältige Diagnose und Therapie mit dem Ziel der Heilung des Patienten. Eine Verfälschung, Unvollständigkeit oder Inkonsistenz medizinischer Daten kann zu falschen medizinischen Entscheidungen mit unter Umständen lebensbedrohenden Folgen für den Patienten führen, verbunden mit rechtlichen Konsequenzen für den Mediziner.

Den Integritätsmerkmalen Gültigkeit und Widerspruchsfreiheit kommen in Bezug auf elektronische Patientenakten eine besondere Bedeutung zu. Integritätsschutz bedeutet mehr als nur die Verhinderung bzw. die Erkennung von syntaktischen Veränderungen einzelner Datenobjekte, sondern zielt auch auf die semantische Gültigkeit und Konsistenz des Datenbestandes in seiner Gesamtheit ab und ebenso auf die semantische Integrität der durch die Zugriffsberechtigungen definierten Teilsichten auf die Akte. Eine elektronische Patientenakte ist das informatorische Abbild des Gesundheitszustandes und der Krankengeschichte eines Patienten. Widersprüchlichkeiten, nicht mehr gültige Daten oder zu Verzerrungen führende Sichten, führen zu einer Informationsbasis, die als Behandlungsgrundlage nicht verlässlich und damit für Arzt und Patient in mehrfacher Hinsicht gefährlich ist. Die

Aufrechterhaltung bzw. Wiederherstellung eines semantisch integren Datenbestandes ist primär eine medizinisch-fachliche Aufgabe, die mit technischen Mechanismen nicht zu bewerkstelligen ist.

2.2.2 Grundlegende Anforderungen zur Integritätssicherstellung

2.2.2.1 Syntaktische Integrität der medizinischen Datenobjekte

Informationsobjekt	Medizinisches Datenobjekt (MDO)
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18-So019)
Kernanforderungen	
Int-MDO-01	Die Unversehrtheit der medizinischen Datenobjekte ist durchgängig vom Erzeuger des Objekts bis zum Nutzer des Objekts sicherzustellen.
Int-MDO-02	Die Sicherstellung der Integrität erfordert eine Vielzahl von technischen Detailmaßnahmen. Die Gesamtheit der zu treffenden Maßnahmen sind auf der Grundlage eines umfassenden Sicherheitskonzepts zu ermitteln.
Int-MDO-03	Zur Erkennung von Integritätsverletzungen ist für jedes medizinische Datenobjekt der Hashwert seiner Klartextform zu erzeugen. Vor der Präsentation eines MDO für den Nutzer ist der Klartext-Hashwert des MDO zu verifizieren. Schlägt die Verifikation fehl, ist von einer Integritätsverletzung auszugehen.
Int-MDO-04	Außerdem ist für jedes medizinische Datenobjekt der Hashwert seiner verschlüsselten Form zu erzeugen. Vor der Entschlüsselung eines MDO ist sein Kryptogramm-Hashwert zu verifizieren. Schlägt die Verifikation fehl, wird der Prozess mit einer Fehlermeldung abgebrochen und die Entschlüsselung wird nicht durchgeführt.
Int-MDO-05	Welche Hashfunktionen verwendet werden, richtet sich nach den Empfehlungen des BSI.
Anmerkungen 1.	Grundsätzlich ermöglicht das Hashwert-Verfahren nur die Erkennung der Veränderung eines Datenobjekts. Die Verhinderung einer Veränderung erfordert eine Vielzahl von Maßnahmen. Dazu gehören die korrekte Funktionsweise von Soft- und Hardware sowie hinreichende Sicherheitsmaßnahmen zur Verhinderung böswilliger Manipulationen. In letzter Konsequenz ist eine Datenveränderung mit technischen Mitteln nicht zu verhindern, da auch nicht kontrollierbare Störeinflüsse - beispielweise elektromagnetischer Art - Manipulationen bewirken können. 2. Schlägt die Verifikation des Hashwertes des verschlüsselten MDO fehl, muss man von einer Veränderung des Schlüsseltextes ausgehen. Würde man nun das MDO entschlüsseln und dann den Hashwert des Klartextes verifizieren, sollte dies fehlschlagen. Es kann aber auch die Situation eintreten, dass der veränderte Schlüsseltext nach seiner Entschlüsselung zu einem Klartext führt, der mit dem originalen Klartext eine Kollision erzeugt. Damit würde die Verifikation des Hashwerts des entschlüsselten Textes erfolgreich sein, obwohl der Schlüsseltext verändert wurde. Abhängig von dem gewählten Verschlüsselungsverfahren bzw. dem Verschlüsselungsmodus und dem Umfang der Veränderung des Schlüsseltextes, sind die

	Veränderungen im entschlüsselten Text nur partiell und eventuell vom Nutzer nicht erkennbar (beispielweise bei Bildinformationen). Insofern ist sicherheitshalber sowohl der Hashwert des Klartextes als auch der des Schlüsseltextes zu erzeugen und zu verifizieren. 3. Anforderung Int-MDO-03 wird nicht - wie oft behauptet - als Nebeneffekt von der elektronischen Signatur abgedeckt. Schlägt nämlich die Verifikation einer elektronischen Signatur fehl, ist nicht entscheidbar, ob das betreffende Datenobjekt manipuliert wurde oder ob das Datenobjekt nicht von dem angenommen Urheber signiert wurde.
Folgerungen	Bei der Verwendung von Hashverfahren bleibt wegen der grundsätzlichen Möglichkeit von Kollisionen ein Restrisiko, das schwer einzuschätzen ist. Kryptologen warnen davor, mit Hashverfahren zu sorglos umzugehen (siehe beispielweise www.cits.rub.de/MD5Collisions). Unter dem Aspekt, dass die Integrität der MDOs einem sehr hohen Schutzbedarf unterliegt, sollte man sehr vorsichtig vorgehen und Datenobjekte, bei denen Veränderungen der Mensch schwer feststellen kann, nicht in eine EPA aufnehmen. Denn es ist nicht mit letzter Sicherheit gewährleistet, dass ein manipuliertes MDO zu einem anderen Hashwert führt als das originale MDO.

2.2.2.2 Integrität der eingesetzten Software

Objekt	Medizinische Software (MSW) Unter medizinischer Software sollen alle Softwarekomponenten (sowohl auf Seiten der Server- als auch der Clientsysteme) verstanden werden, die eine Funktion bei der Verarbeitung von EPA-Daten haben.
Schutzbedarfsstufe	**sehr hoch** Begründung: • Fehlerhafte bzw. manipulierte Software kann dazu führen, dass Daten verändert oder Funktionen nicht ihrer Bestimmung nach ausgeführt werden, mit der Konsequenz, dass Patienten falsch behandelt werden mit u.U. gravierenden Folgen für Leib und Leben.
Kernanforderungen	
Int-MSW-01	Zur Erkennung von Manipulationen an der eingesetzten Software sind die einzelnen Programmkomponenten vom Hersteller der Software mit ihren signierten Hashwerten auszuliefern. Es muss ein Systemmechanismus vorhanden sein, der vor einem Aufruf einer Programmkomponente deren Hashwert und Signatur verifiziert. Schlägt die Verifikation fehl, ist die Programmausführung abzubrechen.
Int-MSW-02	Mittelfristig ist anzustreben, nur noch zertifizierte Software für den Einsatz in EPA-Systemen zuzulassen.

2.2.2.3 Semantische Integrität der EPA

Informationsobjekt	**Elektronische Patientenakte in ihrer Gesamtheit (EPA)**
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18-So019)
Kernanforderungen	
Int-EPA-01	Für jede EPA muss es einen Heilberufler geben, der die semantische Integrität der EPA in ihrer Gesamtheit unter medizinisch-fachlichen Aspekten sicherstellt und damit im Rechtssinne verantwortet. Dazu gehört die Aufrechterhaltung bzw. Wiederherstellung eines konsistenten Zustands sowie die Überprüfung der definierten Sichten und die Einrichtung neuer Sichten.
Int-EPA-02	Dieser Heilberufler muss einen Vollzugriff auf die EPA haben, sowohl bezogen auf die auf den MDOs durchführbaren Operationen als auch bezogen auf die Operationen zur Rechteverwaltung.
Int-EPA-03	Der Heilberufler wird vom Patienten bestimmt und autorisiert.
Int-EPA-04	Der Heilberufler darf Änderungen, die er für notwendig hält, nur mit Zustimmung des Patienten durchführen.
Int-EPA-05	Hält der Heilberufler eine Änderung für dringend erforderlich und stimmt der Patient der Durchführung nicht zu, ist in minder schweren Fällen dieser Umstand schriftlich festzuhalten und vom Patienten zu unterschreiben. In schweren Fällen ist für den Heilberufler ein Recht auf Sperrung der gesamten EPA vorzusehen. Dieses Verfahren ist insgesamt gesetzlich zu regeln.

2.3 Gewährleistung der Verfügbarkeit

2.3.1 Definition Verfügbarkeit

Die Verfügbarkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. personenbezogene Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Die zeitgerechte Verfügbarkeit medizinischer Informationen kann entscheidend sein für eine erfolgreiche Erfüllung des Behandlungsauftrags. Nicht oder nicht rechtzeitig zur Verfügung stehende Daten können zur Handlungsunfähigkeit bzw. zu einem zu späten Handeln oder Behandlungsfehlern des Mediziners führen und u.U. lebensbedrohende Folgen für den Patienten sowie rechtliche Konsequenzen für den Mediziner haben. Die Verfügbarkeit der Daten impliziert natürlich die Verfügbarkeit der zur ordnungsgemäßen Verarbeitung erforderlichen Komponenten (Hard- und Software) des IT-Systems.

2.3.2 Grundlegende Anforderungen zur Gewährleistung der Verfügbarkeit

Objekte	**EPA-Daten, Software, Hardware (ESH)**
Schutzbedarfsstufe	**hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18-So018)
Kernanforderungen	
Verf-ESH-01	Die zu treffenden Maßnahmen entsprechen im Wesentlichen denen, die auch bei anderen IT-Systemen mit Hochverfügbarkeitsanforderungen zu treffen sind. Welche Maßnahmen dies im Detail sind, ist im Rahmen eines Sicherheitskonzepts für eine konkrete Systemrealisierung festzulegen. Anmerkung: • Die Verfügbarkeit eines Systems wird stark beeinflusst von seiner Komplexität. Mit zunehmender Systemkomplexität steigt auch das Risiko des Verlusts der Verfügbarkeit einzelner Systemkomponenten. Anzustreben ist somit bereits im Systementwurf eine Reduzierung der Komplexität. • Aus Nutzersicht ist die Verfügbarkeit eines Systems auch abhängig von den Faktoren Alltagstauglichkeit, Praktikabilität und Bedienungsfreundlichkeit. Ein System, dass hier Defizite aufweist, mag zwar technisch verfügbar sein, wenn aber der Umgang mit dem System zu kompliziert ist, dann ist für die Nutzer die Systemverfügbarkeit faktisch eingeschränkt.
Verf-ESH-02	Die Wiederherstellung von MDOs, die beispielsweise aufgrund einer Integritätsverletzung ihre Verfügbarkeit verloren haben, muss möglich sein. <u>Lösungsmöglichkeit:</u> Die Wiederherstellung eines MDO kann durch erneute Anforderung des MDO von seiner Quelle (lieferndes Primärsystem) realisiert werden. Dazu muss das Original-MDO aber im jeweiligen Primärsystem referenzierbar sein. Dies wird möglich, wenn dem Primärsystem nach einem Daten-Upload die vom EPA-System vergebene interne OID des eingestellten MDO mitgeteilt wird. Das Primärsystem muss dann die OID zusammen mit

		dem gesendeten MDO in seiner verschlüsselten Form speichern. Verschlüsselt deshalb, weil in die EPA nur verschlüsselte Dokumente eingestellt werden und eine erneute Verschlüsselung bei nachträglicher Anforderung u.U. nicht mehr möglich ist. Das Verfahren zur Mitteilung der OIDs an die Primärsysteme kann mit dem Quittungsverfahren zur Nicht-Abstreitbarkeit verbunden werden (siehe entsprechenden Abschnitt).
Verf-ESH-03		Es ist ein Notfallkonzept für den Fall von Verfügbarkeitsverlusten zu erarbeiten.

2.4 Gewährleistung der Zurechenbarkeit

2.4.1 Definition Zurechenbarkeit

Die Zurechenbarkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. der Urheber von patientenbezogenen bzw. der Verantwortliche für patientenbezogene Daten sowie der Auslöser eines Verarbeitungsvorgangs bzw. der Verantwortliche für einen Verarbeitungsvorgang muss jederzeit eindeutig feststellbar sein.

Medizinische Dokumente, die ihren Urheber bzw. Verantwortlichen nicht erkennen lassen, sind als Grundlage für Behandlungen ungeeignet. Ebenso müssen medizinische Dokumente eindeutig und zweifelsfrei einem Patienten zugeordnet werden können. Dies setzt voraus, dass Mediziner und Patienten eindeutig identifizierbar und authentifizierbar sind. Darüber hinaus muss jeder Verarbeitungsprozess eindeutig seinem Auslöser zugeordnet werden können. Die Sicherstellung der Zurechenbarkeitsanforderung ist eine notwendige Voraussetzung für die Gewährleistung der Revisionsfähigkeit.

2.4.2 Grundlegende Anforderungen zur Gewährleistung der Zurechenbarkeit

2.4.2.1 Identifizierung und Authentifizierung von Patienten

Objekt	**Identität und Authentizität des Patienten (Pat)**
Schutzbedarfsstufe	**sehr hoch** Begründung: Die Identität und Authentizität eines Patienten ist eine notwendige Voraussetzung, eine Zuordnung zwischen einer EPA und deren MDOs zur richtigen Person treffen zu können. Da die Schutzbedarfsanforderung für diese Zuordnung sehr hoch ist, ergibt sich damit auch der sehr hohe Schutzbedarf für die Identifizierung und Authentifizierung des Patienten.
Kernanforderungen	
IdAu-Pat-01	Ein Patient muss durch einen Heilberufler eindeutig identifiziert und authentifiziert werden. Dies kann nur manuell auf der Grundlage eines amtlichen Dokuments (wie Personalausweis oder Krankenversichertenkarte), das biometrische Merkmale (wie Bild und Unterschrift) enthält, durchgeführt werden. Ausnahme: Der Patient ist dem Heilberufler persönlich bekannt.

2.4.2.2 Identifizierung und Authentifizierung von Heilberuflern

Objekt	**Identität und Authentizität des Heilberuflers (HB)**
Schutzbedarfsstufe	**sehr hoch** Begründung: • Die Identität und Authentizität eines Heilberuflers ist die notwendige Voraussetzung zur Gewährleistung der Zurechenbarkeit eines Verarbei-

	tungsprozesses zu dessen Auslöser. Da für diese Zurechenbarkeit ein sehr hoher Schutzbedarf gefordert ist, ergibt sich zwangsläufig der sehr hohe Schutzbedarf für die Identität und Authentizität der Heilberufler.
Kernanforderungen	
IdAu-HB-01	Die Authentifizierung erfolgt auf der Grundlage von Smartcards (Heilberufeausweis) und basiert auf Besitz und Wissen oder Besitz und biometrischen Merkmalen.
IdAu-HB-02	Das Authentifizierungsprotokoll basiert auf einem kryptographischen, zertifikatsbasierten challenge response Verfahren.
IdAu-HB-03	Die Zertifikate werden von einer vertrauenswürdigen Stelle ausgestellt, die den Heilberufler als Person und in seiner beruflichen Stellung identifiziert und authentifiziert hat.
IdAu-HB-04	Die Authentifizierung erfolgt gegenüber einem vertrauenswürdigen Authentifizierungsdienst.
IdAu-HB-05	Der Authentifizierungsdienst stellt dem authentifizierten Heilberufler ein mit einem Gültigkeitszeitraum versehenes Zugriffszertifikat (Ticket) zur berechtigten Nutzung eines EPA-Dienstes aus. Das Ticket ist vom Authentifizierungsdienst signiert.
IdAu-HB-06	Bei einem Zugriff auf den EPA-Dienst wird das vom Authentifizierungsdienst ausgestellte Ticket verwendet.
IdAu-HB-06	Das Primärsystem muss über sichere Mechanismen zur Speicherung und eindeutigen Zuordnung des Tickets zu seinem Besitzer verfügen. Die Mechanismenstärke muss dem Schutzbedarf „sehr hoch“ gerecht werden.
Anmerkung	In Gesprächen mit Ärzten wurde deutlich, dass eine Authentifizierung bei jedem Zugriff auf den EPA-Dienst nicht akzeptiert wird. Die Erfüllung dieser Anforderung erfordert die Einführung von Tickets mit einem Gültigkeitszeitraum. Die Authentifizierung gegenüber dem EPA-Dienst erfolgt dann auf der Grundlage dieser Tickets. Hieraus ergibt sich ein Problem. Dieses zweistufige Verfahren erfordert, dass die Zuordnung eines Tickets zu seinem Besitzer im Primärsystem erfolgt. Der Mechanismus, der die Zurechenbarkeit der Tickets zu ihren Besitzern realisiert, muss entsprechend dem sehr hohen Schutzbedarf für die Authentizität der Heilberufler, eine Mechanismenstärke von sehr hoch aufweisen. Lässt sich diese Anforderung technisch nicht umsetzen, muss man zwangsläufig ein einstufiges Verfahren wählen, welches die Authentifizierung gegenüber dem Authentifizierungsdienst und die anschließende Anmeldung mit dem Ticket beim EPA-Dienst innerhalb einer Transaktion sicherstellt. Dies würde aber bedeuten, dass bei jedem Zugriff eine erneute Authentifizierung erfolgen muss.

2.4.2.3 Zurechenbarkeit eines medizinischen Datenobjekts zu seinem Urheber bzw. zu dem für den Inhalt verantwortlichen Heilberufler

Objektbeziehung	**MDO → Urheber/Verantwortlicher (MDO_U)**

Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18-So019)
Kernanforderungen	
Zur-MDO_U-01	Jedes medizinische Datenobjekt ist von seinem Ersteller bzw. von dem für den Inhalt Verantwortlichen mit dessen elektronischer Signatur zu versehen.
Zur-MDO_U-02	Die Signatur muss die gesetzlichen Anforderungen an eine qualifizierte elektronische Signatur erfüllen.
Zur-MDO_U-03	Jedes medizinische Datenobjekt ist mit einem Zeitstempel zu versehen.
Zur-MDO_U-04	Der Zeitstempel muss aus einer vertrauenswürdigen Quelle stammen.
Anmerkung	Wegen der Schutzbedarfsstufe „sehr hoch“ ist die qualifizierte Signatur zu fordern, denn nur sie basiert auf einem qualifizierten Zertifikat und nur für sie fordert das Signaturgesetz eine sichere Signaturerstellungseinheit.

2.4.2.4 Zurechenbarkeit eines medizinischen Datenobjekts zum Patienten

Objektbeziehung	**MDO → Patient (MDO_P)**
Schutzbedarfsstufe	**sehr hoch** Begründung: • Wird ein medizinisches Datenobjekt einem Patienten zugeordnet, auf den es sich inhaltlich nicht bezieht, kann es zu einer Fehlbehandlung dieses Patienten kommen, mit u.U. schwerwiegenden Folgen für Leib und Leben.
Kernanforderungen	
Zur-MDO_P-01	Jedes medizinische Datenobjekt muss die identifizierenden Daten (Stammdaten) des Patienten enthalten, auf den es sich inhaltlich bezieht.
Zur-MDO_P-02	Der Ersteller des MDO muss sich vergewissern, dass der Stammdateneintrag auch zu dem Patienten gehört, auf den sich das MDO inhaltlich bezieht.
Anmerkung	Die Stammdaten des Patienten sind damit Teil des atomaren Informationsobjekts MDO und durch die Signatur mit der inhaltlichen Aussage gekapselt.

2.4.2.5 Zurechenbarkeit der EPA zum Patienten

Objektbeziehung	**EPA → Patient (EPA_P)**
Schutzbedarfsstufe	**sehr hoch** Begründung: • Werden Operationen (Einstellen von MDOs, Einrichten oder Ändern von Berechtigungen etc.) auf der EPA eines Patienten durchgeführt, der nicht

	der angenommene Patienten ist, entstehen in beiden EPAs (nämlich in der falschen und in der, auf die sich die Operationen eigentlich beziehen sollten) inkonsistente Datenbestände bzw. Sichten. Dies kann Falschbehandlungen mit u. U. lebensbedrohenden Auswirkungen zur Folge haben.
Kernanforderungen	
Zur-EPA_P-01	Jede EPA muss als gesonderten Datensatz die Stammdaten des Patienten enthalten.
Zur-EPA_P-02	Bei einem Zugriff auf die EPA werden dem zugreifenden Benutzer die Stammdaten angezeigt.
Anmerkung	Da eine EPA keinen Rückschluss auf den Patienten ermöglichen darf, (siehe Anforderungen zum EPA-Identifikator) müssen die Stammdaten des Patienten verschlüsselt in der EPA abgelegt werden. Das hierzu gewählte kryptographische Verfahren muss eine Ende-zu-Ende (Person-zu-Person) Vertraulichkeit gewährleisten. Das heißt, derjenige Heilberufler, der eine EPA für einen Patienten neu anlegt, erzeugt den verschlüsselten Stammdatensatz. Eine Entschlüsselung darf nur einem autorisierten Heilberufler möglich. Hinweis: Die Anforderungen an das kryptographische Verfahren zur Verschlüsselung der Stammdaten, entsprechen denen zur Verschlüsselung der MDOs. Man kann hier also ein und dasselbe Verfahren verwenden.

2.4.2.6 Zurechenbarkeit eines Verarbeitungsprozesses zu dessen Auslöser

Objektbeziehung	**Verarbeitungsprozess → Auslöser (VP_A)**
Relevante Verarbeitungsprozesse:	
1.	Anlegen einer Akte (open EPA)
2.	Einstellen eines MDO (insert MDO)
3.	Ändern eines MDO (update MDO)
4.	Löschen eines MDO (delete MDO)
5.	Auflisten der Metadaten zu MDOs (list Meta)
6.	Sperren eines MDO (lock MDO)
7.	Entsperren eines MDO (unlock MDO)
8.	Schließen einer Akte (close EPA)
9.	Zuweisen einer Berechtigung (grant right)
10.	Entziehen einer Berechtigung (revoke right)
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18-So019)
Kernanforderungen	
Zur-VP_A-01	Verarbeitungsprozesse dürfen nur ausgelöst werden, wenn der Auslöser ein gültiges Zertifikat vorweisen kann, dass er aufgrund eines sicheren Au-

994 995 996		thentifizierungsprozesses erhalten hat und seine eindeutige Identifizierung ermöglicht. Der Authentifizierungsprozess muss die Schutzstufe „sehr hoch“ erfüllen.

2.5 Gewährleistung der Nutzungsfestlegung

2.5.1 Definition Nutzungsfestlegung

EPA-Systeme müssen es ermöglichen, für jedes patientenbezogene Informationsobjekt abgestufte Nutzungsrechte und Nutzungsausschlüsse zu definieren und sie müssen gewährleisteten, dass eine Datennutzung nur in einem konkreten Behandlungskontext erfolgen kann.

Nach dem verfassungsrechtlichen Erforderlichkeitsgrundsatz dürfen die Daten einer elektronischen Patientenakte nur in einem Umfang genutzt werden, wie es für die jeweilige Behandlungssituation notwendig ist. Dies bedeutet, dass bei einem Zugriff eine konkrete Behandlungssituation vorliegen muss und der Zugriff sich nur auf die Daten beschränkt, die zur Erfüllung dieses Behandlungsauftrags erforderlich sind.

Umsetzen lässt sich eine solche Anforderung nur mit Kontext-basierten Berechtigungsstrukturen als Zusammenfassung von Subjekten und Ressourcen mit Bedingungen. Zum Beispiel: Der Internist A darf auf die internistisch relevanten Daten der EPA des Patienten A zugreifen, solange er in einem konkreten Behandlungskontext zu Patient A steht. Zur Umsetzung solcher Berechtigungsstrukturen benötigt man einerseits ein Rollen-basiertes und Identitäten-basiertes Berechtigungskonzept, verbunden mit der Möglichkeit zur Datenkategorisierung. Andererseits müssen die Rollen bzw. die Identitäten parametrisierbar sein, zur Festlegung eines Behandlungsbeginns und eines Behandlungsendes in Bezug auf eine bestimmte Identität Patient.

2.5.2 Grundlegende Anforderungen zur Gewährleitung der Nutzungsfestlegung

2.5.2.1 Nutzungsrechte für die medizinischen Datenobjekte und Metadaten einer EPA

Informationsobjekt	**Medizinisches Datenobjekt und Metadatum (MDO_Meta)**
Schutzbedarfsstufe	**hoch** Begründung: • Wenn ein EPA-System die Umsetzung des Erforderlichkeitsgrundsatzes nicht gewährleisten kann, werden die betroffenen Patienten grundlegend in ihrem Recht auf informationellen Selbstbestimmung beeinträchtigt. Der Umgang mit ihren Daten ist dann durchweg rechtswidrig. • Eine rechtswirksame Einwilligung zur Nutzung von EPA-Daten basiert u. a. auf einer Differenzierung des Nutzungszwecks (Grundsatz der Zweckbindung); Pauschaleinwilligungen sind rechtsunwirksam. Wenn ein EPA-System keine Mechanismen zur Umsetzung der Nutzungsdifferenzierung bereitstellt, ist die damit verbundene Datenverarbeitung rechtswidrig.
Kernanforderungen	
Nu-MDO_Meta-01	Es muss die Möglichkeit gegeben sein, medizinische Datenobjekte und deren Metadaten zu Kategorien zusammenzufassen.
Nu-MDO_Meta-02	Für die Objekte einer Kategorie müssen sowohl Rollen- als auch Identitäten-basierte Zugriffsrechte vergeben werden können. Die Mitwirkung der Patienten ist dabei zu gewährleisten.

Nu-MDO_Meta-03	Es ist ein Identitäten- und Rollenmanagement zu realisieren. Die Identitäten mit den zugehörigen Rollen sollten dezentral in den jeweiligen medizinischen Einrichtungen spezifizierbar sein.
Nu-MDO_Meta-04	Es muss ein Mechanismus vorhanden sein, der das Vorliegen eines Behandlungskontextes zwischen einer Identität (Heilberufler) und dem Besitzer der EPA erkennt. Lösungsidee: Die Erkennung eines Behandlungskontextes könnte folgendermaßen realisiert werden: Wenn der EPA-Identifikator im Besitz des Patienten ist (siehe Kapitel 3.1.2 (3)), kann ein Heilberufler nur auf dessen EPA zugreifen, wenn ihm der Identifikator vom Patienten mitgeteilt bzw. ausgehändigt wird. Der EPA-Identifikator könnte nun um eine Transaktionskomponente erweitert werden. Der Patient würde dann neben dem Identifikator eine einmalige Transaktionsnummer übergeben. Diese Transaktionsnummer wird vom Berechtigungssystem bei erstmaligem Zugriff mit der Identität des zugreifenden Heilberuflers verbunden und mit einer Gültigkeitsdauer (evtl. abhängig von der Rolle des Heilberuflers) versehen. Greift der Heilberufler nun ein weiteres mal auf die EPA zu, wird die Gültigkeit der Transaktionsnummer validiert. Ist die Gültigkeit abgelaufen, muss der Heilberufler für weitere Zugriffe mit einer neuen Transaktionsnummer durch den Patienten autorisiert werden.
Nu-MDO_Meta-05	Die Autorisierungsprüfung des Zugriffskontrollmechanismus berücksichtigt bei einem Zugriffswunsch folgende Parameter: Zertifikat des Zugreifenden, Identität des Zugreifenden, Rollen des Zugreifenden, und Parameter, der anzeigt, ob sich der Zugreifende in einem Behandlungskontext zum Besitzer der EPA befindet.

2.6 Gewährleistung der Informationsqualität und -validität

2.6.1 Definition Informationsqualität und -validität

Die Qualität und Validität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. personenbezogene Daten müssen aktuell in der für den Nutzungszweck angemessenen Qualität verarbeitet werden können und es muss sichergestellt sein, dass die externe Datendarstellung mit der internen Datenrepräsentation inhaltlich korrekt übereinstimmt.

Die Qualität und Validität medizinischer Daten wird von dem Kriterium der Datenintegrität nicht umfasst. Daten können zwar integer im Sinne von vollständig, gültig und unversehrt sein, die Darstellungsqualität aber dennoch für den jeweiligen medizinischen Nutzungszweck unzureichend sein. Die Validität der Informationsdarstellung ist insbesondere in einer heterogenen Systemlandschaft keine Selbstverständlichkeit. Dieser Umstand ist schon für den Normalnutzer des Internet augenfällig, wenn eine Website mit verschiedenen Browsern betrachtet, ein unterschiedliches Erscheinungsbild aufweist. In der medizinischen Datenverarbeitung, insbesondere bei der Verarbeitung von Daten bildgebender Verfahren, kann eine invalide Datendarstellung erhebliche Konsequenzen haben. Solange die Daten innerhalb einer homogenen, proprietären Systemlandschaft verbleiben, haben Validitätsprobleme noch

keine besondere Bedeutung. Dies ändert sich aber schlagartig, wenn Daten via elektronischer Patientenakten, gegenüber Systemumgebungen geöffnet werden, die auf unterschiedlichen Hardware- Systemsoftware- und Anwendungssoftwareplattformen basieren.

2.6.2 Grundlegende Anforderung an die Informationsqualität und -validität

2.6.2.1 Qualität und Validität medizinischer Datenobjekte

Informationsobjekt	**Medizinisches Datenobjekt (MDO)**
Schutzbedarfsstufe	**sehr hoch** Begründung: • Ist die Darstellung eines MDO in der Qualität für den beabsichtigten Nutzungszweck nicht hinreichend oder ist die Datendarstellung sogar invalide, stützt der Heilberufler seine Entscheidung auf eine Informationsgrundlage, die nicht den realen Gegebenheiten entspricht. Dies kann zu Behandlungsfehlern führen mit u. U. gravierenden Konsequenzen für Leib und Leben des Patienten. • Signiert ein Heilberufler ein MDO, das ihm an der Mensch-Maschine-Schnittstelle nicht valide bezüglich der internen Datenrepräsentation dargestellt wird, bezieht sich seine Willensäußerung in ihrer technischen Umsetzung auf eine andere Sachlage. Entsteht aus diesem Umstand eine Situation, die den Heilberufler in die Beweispflicht dieser Differenz bringt, kann er mit hoher Wahrscheinlichkeit diesen Beweis nicht erbringen.
Kernanforderungen	
QV-MDO-01	Für die systeminterne Repräsentation der MDOs sind Standards für die Datenformate festzulegen.
QV-MDO-02	Für die Präsentation der MDOs an der Mensch-Maschine-Schnittstelle sind sichere Viewer für die unterschiedlichen Systeme und Datenformate zu entwickeln.
QV-MDO-03	Dem Nutzer muss klar sein, in welcher Qualitätsstufe ihm beispielsweise Bilddaten präsentiert werden.
QV-MDO-04	Kommen Verfahren zur Datenkompression zum Einsatz, müssen diese standardisiert sein und die dadurch verursachten Qualitätsverluste müssen quantifizierbar sein.
QV-MDO-05	Die Gesamtproblematik ist detailliert zu analysieren, wozu ein Interoperabilitätskonzept zu erstellen ist.

2.7 Gewährleistung der Revisionsfähigkeit

2.7.1 Definition Revisionsfähigkeit

Die Revisionsfähigkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. die Verarbeitungsprozesse müssen lückenlos nachvollzogen werden können und es muss feststellbar sein, wer wann welche patientenbezogenen Daten auf welche Weise verarbeitet hat.

Für den Arzt bzw. das Krankenhaus besteht nach der Berufsordnung (§ 10 M-BO) die Pflicht zur Dokumentation der Behandlung. Sie ist zudem eine unselbständige Nebenpflicht aus dem Behandlungsvertrag. Eine lückenhafte Dokumentation kann im Haftungsprozess eine Beweislastumkehr zugunsten des Patienten nach sich ziehen. Es muss nachvollziehbar sein, wer welche Diagnose gestellt und welche Therapie verordnet hat und aufgrund welcher Informationen ein Arzt seine Entscheidung über Behandlungsmaßnahmen getroffen hat bzw. ihm mit der Möglichkeit der Kenntnisnahme vorgelegen hat. Eine notwendige Voraussetzung für die Gewährleistung der Revisionsfähigkeit ist die Sicherstellung der Zurechenbarkeit.

2.7.2 Grundlegende Anforderungen an die Revisionsfähigkeit

2.7.2.1 Protokollierung der Verarbeitungsprozesse

Objekt	**Verarbeitungsprozess (VP)**
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18 – So019)
Kernanforderungen	
Rev-VP-01	Jede Operation auf einem Informationsobjekt ist mit dem Zeitpunkt der Operation und dem Zertifikat des Auslösers der Operation zu protokollieren. <u>Relevante Operationen:</u> 1. Anlegen einer Akte (open EPA) 2. Einstellen eines MDO (insert MDO) 3. Lesen eines MDO (read MDO) 4. Ändern eines MDO (update MDO) 5. Löschen eines MDO (delete MDO) 6. Auflisten der Metadaten zu MDOs (list Meta) 7. Sperren eines MDO (lock MDO) 8. Entsperren eines MDO (unlock MDO) 9. Schließen einer Akte (close EPA)
Rev-VP-02	Jede Zuweisung und jeder Entzug einer Berechtigung für ein Informationsobjekt ist mit Zeitpunkt und dem Zertifikat des Auslösers der Berechtigungsoperation zu protokollieren. <u>Relevante Operationen:</u> 1. Zuweisen einer Berechtigung (grant right) 2. Entziehen einer Berechtigung (revoke right)

Rev-VP-03	Die Informationsobjekte werden repräsentiert durch eine eindeutige OID.
Rev-VP-04	Die protokollierten Zeitpunkte basieren auf einem Zeitstempel, der von einer vertrauenswürdigen Quelle stammt. Anmerkung: Die Quelle ist dann vertrauenswürdig, wenn sie im Sinne des Schutzbedarfs „sehr hoch“ eine korrekte Zeit liefert. Welche technische Lösung hier zu wählen ist, hängt von der konkreten Implementierung ab. Denkbar ist die Nutzung eines systemweit zur Verfügung stehenden Zeitdienstes oder aber auch die Nutzung von Funkuhren, die in die Client-Systeme eingebaut werden.

2.7.2.2 Erstellung einer Aktenhistorie

Objekt	**EPA-Version (EPA_V)**
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18 – So019)
Kernanforderungen	
Rev-EPA_V-01	Für jeden beliebigen Zeitpunkt ist der zu diesem Zeitpunkt gültige Zustand einer EPA rekonstruierbar. Das heißt alle MDOs und deren Metadaten, die potentiell zu diesem Zeitpunkt im Zugriff standen (d.h. nicht gelöscht und nicht gesperrt waren) sowie die zu diesem Zeitpunkt gültigen Zugriffsrechte.
Anmerkung	Der Zustand einer EPA zu einem bestimmten Zeitpunkt ist rekonstruierbar über die Auswertung der Protokolldaten bis zu diesem Zeitpunkt.

2.7.2.3 Archivierung einer elektronischen Patientenakte

Objekt	**EPA**
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18 – So019)
Kernanforderungen	
Rev-EPA-01	Nach dem Schließen einer EPA ist sie mit allen Informationsobjekten und den Protokolldaten in ein Archiv zu überführen.
Rev-EPA-02	Die Archivierung muss die Anforderungen an eine Langzeitarchivierung erfüllen. Anmerkung: Hierzu ist ein Archivierungskonzept zu erarbeiten. Insbesondere sind dabei folgende Kernfragen zu beantworten: • Wie wird bei ablaufenden Signaturen verfahren (Nachsignatur)? • Wie geht man mit den verschlüsselten MDOs um? Insbesondere ist das Problem der unsicher werdenden kryptographischen Verfahren und Schlüssel zu lösen sowie die Möglichkeit zur Entschlüsselung (wer hat die erforderlichen Schlüssel?).

1212 1213		• Welche Datenformate mit zugehöriger Interpretationssoftware sind zu wählen, um eine Langzeitverfügbarkeit gewährleisten zu können?
1214 1215 1216 1217	Rev-EPA-02	Nach Ablauf der gesetzlichen Aufbewahrungsfrist ist die EPA mit allen Daten physisch zu löschen. Das Löschverfahren muss gewährleisten, dass eine Wiederherstellung der Daten nach dem Stand der Technik nicht mehr möglich ist.

2.8 Gewährleistung der Nicht-Abstreitbarkeit von Datenübermittlungen

2.8.1 Definition Nicht-Abstreitbarkeit von Datenübermittlungen

Die Nicht-Abstreitbarkeit des Sendens und des Empfangs von patientenbezogenen Informationen muss gewährleistet sein. D.h. einerseits ist zu gewährleisten, dass der Sender einer patientenbezogenen Information sicher sein kann, dass die Information ihren Empfänger erreicht hat, und er darf nicht abstreiten können, genau diese Information an genau den Empfänger gesendet zu haben. Andererseits muss der Empfänger einer patientenbezogenen Information sicher sein können, genau diese Information von einem bestimmten Sender empfangen zu haben, und er darf nicht abstreiten können, genau diese Information von einem bestimmten Sender empfangen zu haben.

Die Nicht-Abstreitbarkeit von Datenübermittlungen ist ein Teilaspekt der Revisionsfähigkeit. Wegen ihrer besonderen Bedeutung wird sie an dieser Stelle als eigenständiges Kriterium aufgeführt.

2.8.2 Grundlegende Anforderungen zur Gewährleistung der Nicht-Abstreitbarkeit von Datenübermittlungen

2.8.2.1 Quittungsverfahren

Objekt	**Datenübermittlung (DÜ)**
Schutzbedarfsstufe	**sehr hoch** (Übergreifendes Sicherheitskonzept Gematik C2.18 – So019)
Kernanforderungen	
Rev-DÜ-01	Sendet ein Primärsystem ein MDO an den EPA-Dienst, versieht es dieses mit seiner internen ID (Primär-ID). Nach Eingang des MDO beim EPA-Dienst, stellt dieser eine Eingangsquittung aus. Die Quittung enthält die Primär-ID, die vom EPA-Dienst für dieses Dokument vergebene interne OID, die Hashwerte des MDO (der mitgesendete Kryptogramm-Hashwert und der Klartext-Hashwert) und einen Zeitstempel mit der Eingangszeit. Die Quittung wird vom EPA-Dienst signiert und an das sendende Primärsystem übermittelt. Das Primärsystem speichert die Quittung zusammen mit dem gesendeten (verschlüsselten) MDO. Der EPA-Dienst übernimmt die Quittung zusammen mit der Primär-ID des Primärsystems und dem Zertifikat des Heilberuflers, der den Upload ausgelöst hat, in die Protokolldatei.
Rev-DÜ-02	Sendet das EPA-System ein MDO an ein Primärsystem, versieht es dieses mit der internen OID. Nach Eingang des MDO beim Primärsystem sind vier Fälle zu unterscheiden: 1. Das MDO wird entschlüsselt aber nicht gespeichert 2. Das MDO wird entschlüsselt und gespeichert 3. Das MDO wird nicht entschlüsselt und nicht gespeichert 4. Das MDO wird nicht entschlüsselt aber gespeichert Zu 1: In diesem Fall kann der Inhalt des MDO zur Kenntnis genommen

	werden. Es wird allerdings nicht in das Primärsystem übernommen. Reaktion: Das Primärsystem erstellt eine Lesequittung, indem es die beiden Hashwerte (Klartext- und Kryptogramm-Hashwert) des MDO, die mitgesandte OID und einen Zeitstempel an das EPA-System sendet. Das EPA-System übernimmt die Lesequittung in seine Protokolldatei, zusammen mit dem Zertifikat des Heilberuflers, der den Download initiiert hat. Zu 2: In diesem Fall kann der Inhalt des MDO zur Kenntnis genommen werden und das MDO wurde in das Primärsystem übernommen. Reaktion: Das Primärsystem erstellt eine Lese-/Speicherquittung, indem es die beiden Hashwerte des MDO, die mitgesandte OID, seine intern für dieses MDO vergebene Primär-ID und einen Zeitstempel an das EPA-System sendet. Das EPA-System übernimmt die Lese-/Speicherquittung in seine Protokollierung, zusammen mit dem Zertifikat des Heilberuflers, der den Download ausgelöst hat. Zu 3: In diesem Fall konnten nur die Metadaten des MDO zur Kenntnis genommen werden. Reaktion: Hier genügt die technische Eingangsquittung auf Ebene des DFÜ-Protokolls. Das EPA-System übernimmt diese Quittung mit dem Zertifikat des den Download auslösenden Heilberuflers. Eine Quittung auf Anwendungsebene wird nicht generiert. Zu 4: In diesem Fall konnten zunächst nur die Metadaten zur Kenntnis genommen werden. Das MDO kann aber später noch entschlüsselt werden. Reaktion: Das Primärsystem erstellt eine Speicherquittung, indem es den Kryptogramm-Hashwert des MDO, die mitgesandte OID, seine intern für dieses MDO vergebene Primär-ID und einen Zeitstempel an das EPA-System sendet. Das EPA-System übernimmt die Speicherquittung in die Protokollierung, zusammen mit dem Zertifikat des Heilberuflers, der den Download initiiert hat. Darüber hinaus muss das Primärsystem in der Lage sein, eine Lesequittung an das EPA-System nachzusenden, wenn das verschlüsselt gespeicherte MDO zu einem späteren Zeitpunkt entschlüsselt wird. Diese Lesequittung unterscheidet sich von der des 1. Falles, indem zusätzlich die Primä-ID mitgesandt wird. Das EPA-System führt diese Lesequittung mit der bereits erhaltenen Speicherquittung über die OID + Primär-ID zusammen.
Anmerkung	Das Quittungsverfahren erlaubt die Nachverfolgung eines jeden MDO von seiner Quelle zu den Zielsystemen und eröffnet darüber hinaus eine Möglichkeit zur Wiederherstellung von MDOs durch Anforderung aus den Quellsystemen.

2.9 Gewährleistung der Rechtsverbindlichkeit

2.9.1 Definition Rechtsverbindlichkeit

Für jeden Verarbeitungsvorgang und dessen Ergebnissen ist gegenüber Dritten die verantwortliche bzw. verursachende Instanz beweiskräftig nachweisbar.

Für jeden Verarbeitungsvorgang und dessen Ergebnissen ist der Verursachende bzw. Verantwortliche beweiskräftig nachweispflichtig. Ist die Rechtsverbindlichkeit nicht gegeben, können Patienten eventuelle Schadenansprüche u.U. nicht geltend machen bzw. können Mediziner u.U. die Korrektheit ihres Handelns nicht nachweisen. Die notwendige Voraussetzung für die Gewährleistung der Rechtsverbindlichkeit ist die Gewährleistung der Revisionsfähigkeit. Die Revisionsfähigkeit alleine gewährleistet aber noch nicht die beweiskräftige Überprüfbarkeit von Verarbeitungsvorgängen in gerichtlichen Verfahren.

Da in der digitalen Informationsverarbeitung die Möglichkeit des Augenscheinbeweises nicht gegeben ist, stellt sich die Frage, wie Rechtsverbindlichkeit hergestellt werden kann. Ein erster Schritt sind elektronische Signaturen. Eine Signatur bezieht sich allerdings nur auf einzelne Objekte. Das Problem der Gestaltung rechtsverbindlicher Prozessketten ist damit noch nicht gelöst.

2.9.2 Grundlegende Anforderungen zur Gewährleitung der Rechtsverbindlichkeit

Objekt	**Verarbeitungsvorgänge und deren Ergebnisse (V_E)**
Schutzbedarfsstufe	**hoch** Begründung: • Ist die Rechtsverbindlichkeit nicht gegeben, können u.U. Patienten Schadensansprüche nicht geltend machen, was beachtliche finanzielle Verluste bedeuten könnte. • Kann ein Heilberufler die Korrektheit seines Handelns bezogen auf die ihm zu Zeitpunkt seiner Entscheidungen zur Verfügung gestandene Informationsgrundlage nicht nachweisen, muss er u.U. mit erheblichen Auswirkungen auf seine gesellschaftliche Stellung rechnen bzw. sogar mit rechtlichen Sanktionen.
Kernanforderungen	
Re-V_E-01	Zertifikate zur qualifizierten Signatur der MDOs müssen von **akkreditierten** Zertifizierungsdiensteanbietern ausgestellt werden.
Re-V_E-02	Die elektronische Langzeitarchivierung der EPAs muss beweiskräftig erfolgen.
Re-V_E-03	Die Nachvollziehbarkeit der auf einer EPA durchgeführten Verarbeitungsprozesse muss beweiskräftig sein. Notwendige Voraussetzungen hierfür ist

	die Verwendung von Zertifikaten, die von einer vertrauenswürdigen Dienst ausgestellt wurden.
Anmerkung	Um weitergehende Aussagen machen zu können, sollten die im Projekt ArchiSig gemachten Erfahrungen ausgewertet werden. Darauf aufbauend sollte ein Konzept zur Gewährleistung der Rechtsverbindlichkeit erstellt werden.

2.10 Gewährleistung der Betroffenenrechte

2.10.1 Definition Betroffenenrechtsgarantie

EPA-Systeme sind so zu konzipieren, dass sie technische und/oder organisatorische Mechanismen zur Wahrnehmung der Betroffenenrechte bereitstellen.

Das Recht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen sind nur im überwiegenden Allgemeininteresse zulässig und bedürfen einer verfassungsmäßigen gesetzlichen Grundlage, die dem Gebot der Normenklarheit entspricht und den Verhältnismäßigkeitsgrundsatz beachtet. Insbesondere hat er das Recht auf Auskunft, Berichtigung, Sperrung und Löschung seiner personenbezogenen Daten, sowie auf Schadensersatz und Folgenbeseitigung.

Betroffene sind insoweit in erster Linie die Patientinnen und Patienten sowie die beteiligten Heilberufler. Je nach dem Inhalt der EPA können dies auch weitere Personen sein, wie etwa die Angehörigen und sonstige Personen, die ein Patient im Rahmen der Behandlung genannt und die in der Dokumentation genannt sind. Auf Seiten der Heilberufler gehören hierzu ihre Gehilfen. Die Datenschutzrechte dieses Personenkreises können durchaus miteinander kollidieren. Es wäre auch insoweit notwendig, die absehbaren Konfliktfälle durch generelle Vorgaben in einem Gesetz unter Wahrung der schutzwürdigen Belange der Beteiligten zu lösen.

Die Betroffenenrechte zu garantieren hat die Person(durchweg eine Heilberufler), die die EPA datenschutzrechtlich verantwortet (§ 3 Abs. 7 BDSG). Die Zugriffsmöglichkeiten sind entsprechend auszugestalten. Die letzte Entscheidung für den Umgang mit den Daten der EPA liegt bei ihr. Sie hat gleichzeitig die Aufgabe, die Mitwirkungsrechte und –pflichten der Patienten zu gewährleisten. Ihre Entscheidungen beim Umgang mit der EPA sind im System zu dokumentieren.

2.10.2 Grundlegende Anforderungen zur Gewährleistung der Betroffenenrechte

Objekt	**Rechte der Patienten (RP)**
Schutzbedarfsstufe	**hoch** Begründung: • Wenn ein EPA-System die Wahrnehmung der Rechte der Patienten nicht in vollem Umfang gewährleisten kann, werden die betroffenen Patienten grundlegend in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt. Die Verarbeitung der Daten der Patienten durch ein solches System ist dann durchweg rechtswidrig und ist zu unterlassen.

	Recht auf Auskunft (Ausk)	
	Kernanforderungen	
	RP-Ausk-01	Das EPA-System muss Mechanismen zur Verfügung stellen, so dass die Patienten ihr Recht auf Auskunft wahrnehmen können. Die Mechanismen müssen geeignet sein zur Beantwortung der Frage: Wer hat welche Daten wann und auf welche Weise verarbeitet? Das Auskunftsrecht erstreckt sich damit auf 1. die aktuell „aktive“ Akte, inklusive der eingerichteten Berechtigungen, 2. die Aktenhistorie für jeden beliebigen Zeitpunkt, inklusive der für den jeweiligen Zeitpunkt eingerichteten Berechtigungen, 3. die Protokolldaten mit den Zuständen der MDOs im Zeitablauf und den auf den MDOs durchgeführten Operationen und deren Auslöser und 4. die archivierte Akte nach Schließung der aktiven Patientenakte.
	RP-Ausk-02	Aus Sicht des Patienten muss es eine verantwortliche Stelle zur Durchsetzung seines Auskunftsrechts geben. Das heißt, jeder Patient hat genau einen Ansprechpartner, der seinen Auskunftsanspruch verwirklicht. Die Vertretung muss geregelt sein. <u>Anmerkung</u>: Sollte das EPA-System technische Mechanismen zur Verfügung stellen, die es den Patienten ermöglicht, selbst ihre Auskunftsansprüche zu realisieren, wird dadurch die verantwortliche Stelle nicht obsolet.
	RP-Ausk-03	Das EPA-System muss Mechanismen zur Auswertung, Aufbereitung und patientengerechten Darstellung der Protokolldaten und sonstigen Daten der verantwortlichen Stelle zur Verfügung stellen.
	RP-Ausk-04	Es muss gewährleistet sein, dass die jeweiligen Daten den Patienten in analoger Form zur Verfügung gestellt werden können.
	Anmerkung	Bezieht sich der Auskunftsanspruch auf die Inhalte von MDOs, ist aufgrund der patientenzentrierten Verschlüsselung eine Mitwirkung des Patienten erforderlich, im Sinne einer „Geheimnisübergabe“ an die verantwortliche Stelle. Ebenso ist zu berücksichtigen, dass der verantwortlichen Stelle Daten zu Kenntnis gelangen, die der ärztlichen Schweigepflicht unterliegen.
		Aufgrund dieser Problematik erscheint es am sinnvollsten, dass ein vom Patienten bestimmter Arzt die Aufgaben der verantwortlichen Stelle wahrnimmt. Unter Berücksichtigung der Anforderungen zur Gewährleistung der semantischen Integrität, bietet es sich an, dass beide Aufgaben von ein und demselben Arzt wahrgenommen werden.
		Recht auf Löschung (Del)
	Kernanforderungen	
	RP-Del-01	Das EPA-System muss gewährleisten, dass MDOs mit den zugehörigen Metadaten auf Veranlassung des Patienten gelöscht werden können.

	Hinweis: Eine Löschung darf immer nur logisch erfolgen, nie physisch. Das heißt ein gelöschtes MDO und dessen Metadaten werden der „aktiven“ Akte entzogen und in die Aktenhistorie überführt. In den Protokolldaten ist die Löschung festzuhalten mit Löschzeitpunkt, dem Zertifikat des die Löschung auslösenden Heilberuflers und einem Hinweis, dass die Löschung patientenveranlasst erfolgte.
RP-Del-02	MDOs, die nach 10 Jahren als ärztliche Dokumentation (§ 10 BO) zu löschen wären, sind für den ärztlichen Zugriff zu sperren. Nur der Patient selbst kann diese Daten für eine ärztliche Behandlung freigeben.
RP-Del-03	Das EPA-System muss gewährleisten, dass die Akte spätestens 30 Jahre nach dem Tod, wenn dieser nicht feststellbar ist, 30 Jahre nach dem 80. Geburtstag vollständig gelöscht wird. Der Löschung steht gleich die Abgabe der Akte an ein Archiv, soweit gesetzlich geregelt.
Anmerkung	Das Recht auf Löschung kollidiert u.U. mit der Anforderung nach semantischer Integrität der Akte. Für diesen Fall gelten die Ausführungen zu Anforderung Int-EPA-05 entsprechend. Aus dieser Anforderung resultiert außerdem, dass ein Löschanspruch nur gegenüber dem für die Aufrechterhaltung der semantischen Integrität verantwortlichen Heilberufler (§ 3 Abs.7 BDSG) geltend zu machen ist und dass technische Mechanismen, die es den Patienten selbst ermöglichen, Löschungen in ihren Akten durchzuführen, nicht zur Verfügung stehen dürfen. Dies gilt allerdings nur für den Zeitraum der Dokumentationspflicht (idR 10 Jahre).
	Recht auf Sperrung (Lock)
Kernanforderungen	
RP-Lock-01	Das EPA-System muss Mechanismen zur Sperrung und Entsperrung von MDOs und deren Metadaten bereitstellen. Hinweis: Sperren bedeutet, dass die davon betroffenen MDOs und deren Metadaten in der „aktiven“ Akte verbleiben, aber mit Ausnahme der verantwortlichen Stelle für keinen Nutzer sichtbar und damit auch nicht zugreifbar sind. Ein Entsperren macht sie wieder sichtbar. Eine Sperrung sowie die Entsperrung werden mit Zeitpunkt und dem Zertifikat des die Operation auslösenden Heilberuflers in den Protokolldaten vermerkt. Der Veranlasser einer Sperrung kann immer nur ein Patient sein (kein Heilberufler, im Gegensatz zur Löschung). Ausnahme: die für die EPA verantwortliche Person
RP-Lock-02	Unter Geltung des § 34 StGB muss die verantwortliche Person die Befugnis haben, die EPA vollständig zu sperren. Im Missbrauchsfall und im Streitfall ist die Befugnis zur Entsperrung durch eine Gerichtsentscheidung zu ersetzen (oder durch eine Verpflichtung des Vertreters vorzunehmen).
Anmerkung	Auch das Recht auf Sperren kollidiert u.U. mit der Anforderung nach semantischer Integrität. Die Anmerkungen zur Anforderung RP-Del-01 gelten damit entsprechend.

Hinweis	Eine Entsperrung von MDOs erfordert den Hinweis, dass überhaupt gesperrte Objekte vorliegen, denn diese sind ja nicht sichtbar. Dieser Hinweis ist dem Heilberufler - und nur diesem - anzuzeigen, der verantwortlich für die Durchführung von Sperrungen und Entsperrungen ist. Oder anders ausgedrückt, für diesen Heilberufler bleiben die Objekte sichtbar, tragen aber einen Sperrvermerk. Die einzige Operation, die er auf diesen Objekten aber ausführen kann, ist die Entsperrung. Hierzu benötigt er nach Ablauf von 10 Jahren Speicherdauer für die MDO zwingend die Mitwirkung des Patienten. Für den Patienten sind die gesperrten Objekte immer sichtbar.
	Recht auf Berichtigung
Kernanforderungen	
RP-Ber-01	Das EPA-System muss Mechanismen zur Verfügung stellen, die es den Patienten ermöglichen ihr Recht auf Berichtigung durchsetzen zu können. Unabhängig davon gilt, dass unrichtige Daten zu berichtigen sind. Es handelt sich um eine Kern-Verpflichtung der für die EPA verantwortlichen Person, die diese auch ohne Antrag des Betroffenen durchzuführen hat. Hiervon zu unterscheiden ist der Sonderfall, dass unrichtige Daten nicht berichtigt werden dürfen, da sie den Beweis darstellen für das Vorliegen eines Schadensersatz- oder Folgenbeseitigungsanspruches. Ein weiterer Sonderfall liegt vor, wenn lediglich von dem Betroffenen die Richtigkeit einer Angabe bestritten wird (Dissens mit der verantwortlichen Person). Lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, so sind diese Daten zu sperren. Bis zu dieser "Klärung" ist das Bestreiten der Richtigkeit einer Angabe in geeigneter Weise festzuhalten. Bei einem Zugriff auf diese Angabe ist die Tatsache des Bestritten-Seins immer mit anzuzeigen, es sei denn die schutzwürdigen Belange des Betroffenen verlangen, dass diese Anzeige unterdrückt wird. Die Berichtigung selbst ist begrifflich entweder eine Löschung oder eine Veränderung. Das heißt, dass entweder die unrichtige Angabe unkenntlich gemacht wird und gegebenenfalls an deren Stelle die richtige Angabe gespeichert wird. Die Berichtigung kann auch dadurch bewirkt werden, dass die unrichtige Angabe lediglich als unrichtig gekennzeichnet, d.h. verändert wird, und gegebenenfalls die richtige Angabe hinzugefügt, d.h. zusätzlich gespeichert wird. Welche Vorgehensweise dem Charakter der EPA entspricht, lässt sich im Wege einer Ausschließlichkeit nicht generell festlegen. Zu berücksichtigen ist weiter, dass eine in der EPA festgestellte Unrichtigkeit sich auswirken kann auf die Quelle der Angabe in den Arztpraxen. Ebenso verlangen in den Praxen festgestellte Unrichtigkeiten eine verpflichtende Unterrichtung der verantwortlichen Person unter Übersendung der richtigen Angaben. Die verantwortliche Person hat die betroffenen Patienten zu unterrichten.

	Anmerkung: Eine durch einen Patienten veranlasste Berichtigung, bezieht sich erfahrungsgemäß vorrangig auf eine **bewertende** Aussage innerhalb eines MDO durch den Urheber des MDO, die der Patient nicht hinnehmen möchte (z.B.: „Ich habe den Eindruck, dass Herr Meier medikamentenabhängig ist.“). Im Gegensatz dazu ist eine von einem Heilberufler veranlasste Berichtigung - im Sinne eines Update – häufig als Korrektur einer auf Fakten basierten Aussage zu sehen (z.B.: der angegebene Cholesterinwert von 320 kam aufgrund eines Zahlendrehers zustande und ist tatsächlich 230). Hinzukommen dürften die Berichtigungen, angestoßen durch die verantwortliche Person, die im Zusammenhang mit Zuspeicherungen in die EPA aus unterschiedlichen Quellen stehen, deren Inhalte sich widersprechen oder in sonstiger Weise nicht miteinander im Einklang zu bringen sind.
RP-Ber-02	Die Forderung zur Berichtigung ist gegenüber dem MDO-Urheber als für die Richtigkeit der Quelle verantwortliche Person zu artikulieren. Nur er kann eine Berichtigung durchführen. Der Patient und/oder die für die EPA verantwortliche Person müssen sich also mit dem entsprechenden Heilberufler in Verbindung setzen. Meinungsverschiedenheiten in der Bewertung der Richtigkeit sind kenntlich zu machen und zu klären.
RP-Ber-03	Eine Berichtigung erfolgt, indem das zu berichtigende MDO gelöscht und die berichtigte Version des MDO neu eingestellt wird. Der Patient autorisiert hierzu den Heilberufler durch „Übergabe seines Autorisierungsgeheimnisses“. Ist die Berichtigung aus medizinischer Sicht zwingend notwendig, berichtigt die verantwortliche Person allein und unterrichtet den Betroffenen unverzüglich.
RP-Ber-04	Das aufgrund der Berichtigung gelöschte MDO wird in die Historie übernommen. In der Protokollierung wird es mit Zeitstempel, dem Zertifikat des die Löschung auslösenden Heilberuflers, der OID des neu eingestellten MDO und dem Hinweis auf patientenveranlasste oder durch verantwortliche Person veranlasste Berichtigung erfasst. Weiter ist festzulegen, ob und wie das gelöschte MDO angezeigt wird und wer Zugriff unter welchen Voraussetzungen auf das gelöschte MDO erhalten soll. Dabei sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen.
RP-Ber-05	Wurde das berichtigte MDO bereits in lokale Dokumentationen übernommen, so sind auch dort das berichtigte MDO durch das neue MDO zu ersetzen. Hierzu muss das EPA-System einen Mechanismus vorsehen. Hinweis: Der Berichtigungsmechanismus könnte so realisiert werden, dass über die Protokollierung durch Auswertung der Kommunikationsquittungen ermittelt wird, in welche lokalen Dokumentationen das berichtigte MDO übernommen wurde. Die Quittungen enthalten auch die Zertifikate der Heilberufler, die jeweils den Download ausgelöst haben. An diese Heilberufler ist dann das berichtigte MDO zusätzlich zu senden. Das MDO wird direkt adressiert verschlüsselt, d.h. mit den öffentlichen Schlüsseln der jeweiligen Heilberufler (also HBA-basierte Verschlüsselung). Die verantwortliche Person erhält eine Rückmeldung, wenn die Nachricht von der für die Quelle verantwortli-

	chen Person nicht innerhalb einer angemessenen Frist mit der Möglichkeit zur Kenntnisnahme geöffnet worden ist. Dann ist eine Direktansprache innerhalb und/oder außerhalb des EPA-Systems notwendig.
RP-Ber-06	Die Schaffung einer bereichspezifischen Rechtsgrundlage mit Vorgaben für die Ausübung des Berichtigungsanspruchs und für die Durchführung der Berichtigungsverpflichtung erscheint notwendig.
Anmerkung	Abgrenzung zur Berichtigungen, die durch Heilberufler veranlasst werden: Eine Berichtigung, die durch einen Heilberufler aufgrund der **objektiven Faktenlage** veranlasst wird, unterscheidet sich von der patientenveranlassten Berichtigung im Wesentlichen dadurch, dass zum Berichtigungszeitpunkt in der Regel kein Patientenkontakt mehr besteht. Das bedeutet aber, dass u. U. auf die Akte nicht mehr zugegriffen werden kann. Für solche Fälle muss das EPA-System einen Benachrichtigungsmechanismus vorsehen. Auf dieser Grundlage wird der für die Akte verantwortliche Heilberufler benachrichtigt. Ihm wird das neue MDO direkt adressiert verschlüsselt übermittelt. Da der aktenverantwortliche Heilberufler Vollzugriff auf die Akte hat, kann er die Berichtigung durchführen. Das heißt, er stellt das neue MDO in die Akte ein und "löscht" das überholte MDO. Im Hinblick auf mögliche Haftungsfragen einerseits und Schadensersatzansprüchen der Betroffenen andererseits, sollte für eine Frist von ca. 6 Monaten eine Wiederherstellbarkeit der gelöschten MDO im System vorgesehen sein. Nach Ablauf der Frist erfolgt automatisch die endgültige Löschung. Wurde das überholte MDO bereits von Heilberuflern zur Kenntnis genommen, entscheidet der aktenverantwortliche Heilberufler aufgrund der Faktenlage, ob diese zu informieren sind. Ist dies der Fall, so übermittelt er das neue MDO direkt adressiert verschlüsselt. Das EPA-System muss ihm die Mechanismen zur Ermittlung der Adressaten zur Verfügung stellen (Auswertemechanismen für Protokolle und Kommunikationsquittungen). Darüber hinaus hat der aktenverantwortliche Heilberufler in der Regel den Patienten über die geänderte Sachlage zu informieren. Dies ist im Eigeninteresse der verantwortlichen Person und den möglicherweise im Raum stehenden Haftungsfragen notwendig.

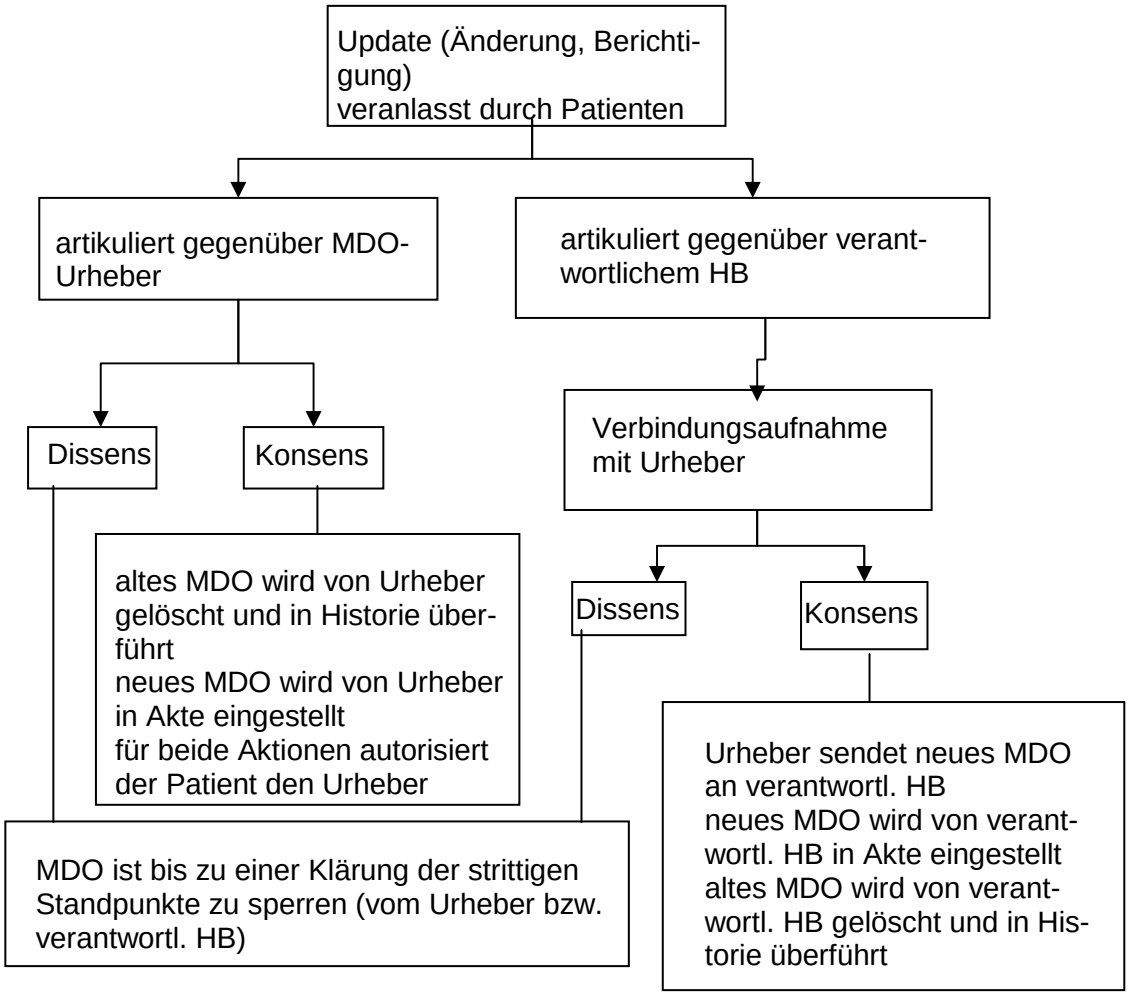
Hinweise zur Berichtigung medizinischer Datenobjekte:

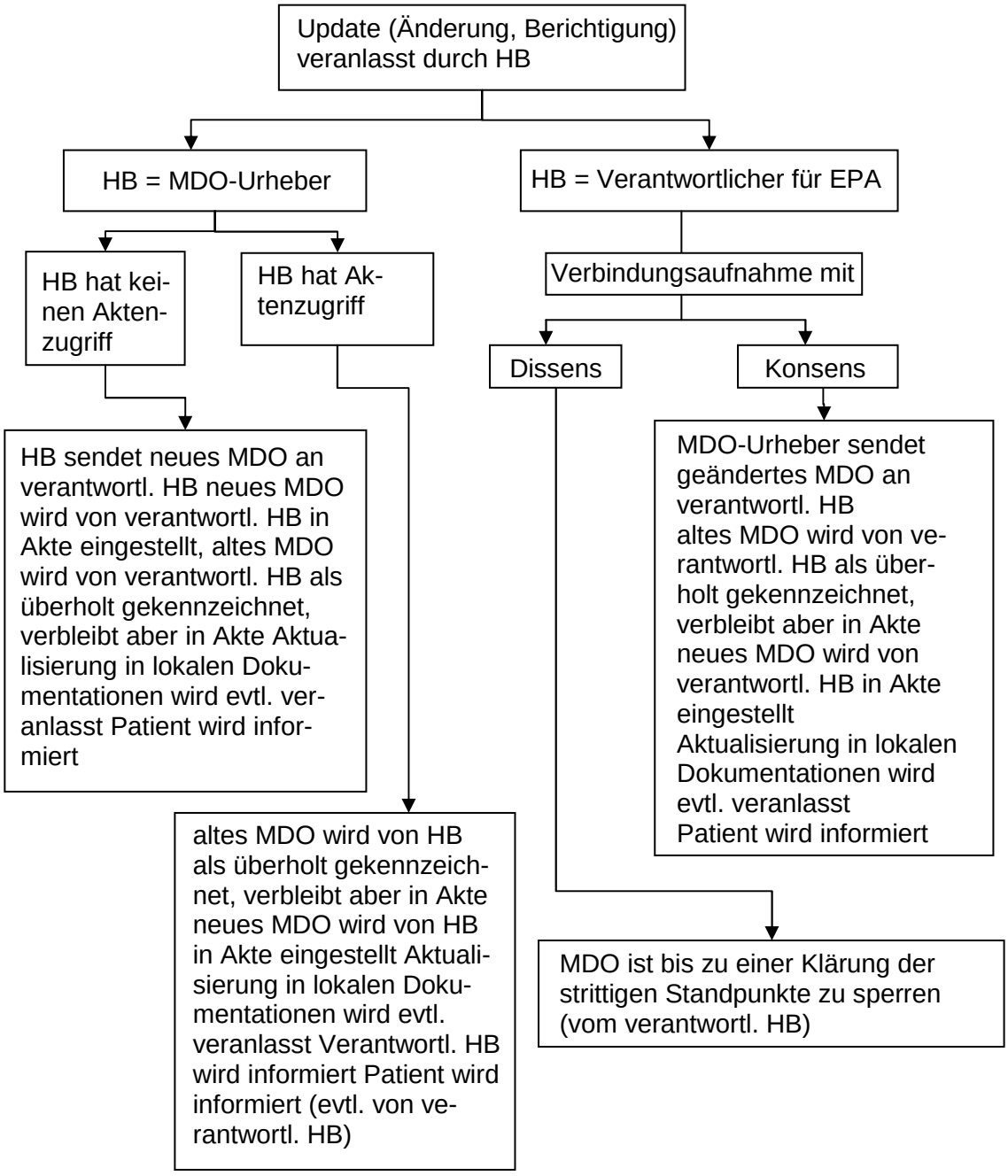
Die Fälle, die eine Berichtigung eines oder mehrer medizinischer Datenobjekte zur Folge haben können, lassen sich grundsätzlich in zwei Kategorien einteilen:

Eine durch einen Patienten veranlasste Berichtigung, die sich vorrangig bezieht auf eine **bewertende Aussage** innerhalb eines MDO durch den Urheber des MDO, die der Patient nicht hinnehmen möchte.

Eine Berichtigung, die durch einen Heilberufler aufgrund der **objektiven Faktenlage** veranlasst wird. Der Initiator kann der Urheber eines Dokuments selbst sein, der für die Akte verantwortliche Heilberufler oder ein weiterer Behandler.

Die folgenden Graphiken sollen die unterschiedlichen auf der Akte durchzuführenden Prozesse für diese beiden Kategorien verdeutlichen:





Anmerkungen zur Gewährleistung der Betroffenenrechte:

Die Umsetzung der Rechte der Patienten auf Löschung, Sperrung und Berichtigung kann einerseits zu Kollisionen mit anderen rechtlichen Anforderungen führen (z.B. dem Haftungsrecht) und andererseits zu Aktenzuständen, die aus medizinisch-fachlicher Sicht nicht vertretbar sind, weil die Akte als Informationsbasis für Behandlungen nicht mehr verlässlich ist oder sogar gefährlich werden kann.

Damit stellt sich die Frage, wie man in der Praxis mit diesem Zielkonflikt umgehen soll? Klar sollte sein, dass die Patienten keinen direkten Zugang zur Akte haben sollten, um Löschungen Sperrungen

oder Berichtigungen eigenständig durchzuführen. Es muss jemanden geben, der sie berät und auf die möglichen Folgen hinweist. Dies kann aber nur ein Heilberufler sein, da die Bewertung der potentiellen Auswirkungen einer medizinisch-fachlichen Beurteilung bedarf. Hier bietet sich der Heilberufler an, der unter dem Aspekt der Aufrechterhaltung der semantischen Integrität die Akte pflegen muss. Dieser Arzt wäre damit der Vertrauensarzt in Sachen Patientenakte. Offen bleibt dann noch, wie verfahren werden soll, wenn zwischen dem Vertrauensarzt und dem Patienten kein Konsens erzielt werden kann. Eine denkbare Vorgehensweise könnte sein, dass in Fällen, die minderschwere Auswirkungen zur Folge haben können, die Ansprüche der Patienten umgesetzt werden und der Arzt sich die veranlassten Änderungen vom Patienten schriftlich bestätigen lässt. Für Fälle, die das Potential schwerer Auswirkungen in sich bergen, könnte man eine Schiedsstelle einrichten oder aber auch dem verantwortlichen Arzt das Recht einräumen, die gesamte Akte zu sperren. Dies müsste allerdings über den Einzelfall hinaus generell gesetzlich geregelt werden.

2.11 Gewährleistung der Alltagstauglichkeit

2.11.1 Definition Alltagstauglichkeit

EPA-Systeme sind so zu konzipieren, dass sie die medizinischen Behandlungsprozesse und die organisatorischen Abläufe in den medizinischen Einrichtungen in adäquater Weise unterstützen.

EPA-Systeme sind kein Selbstzweck, sondern sie sollen ein Mittel zur Verbesserung der Behandlungsqualität und zur Erhöhung der Wirtschaftlichkeit der medizinischen Behandlung sein. Diese Ziele sind aber nur erreichbar, wenn die mit EPA-Systemen verbundenen technischen Abläufe, die sich aus den medizinischen Behandlungsprozessen ergebenden Anforderungen adäquat abbilden und darüber hinaus die organisatorischen Gegebenheiten in den medizinischen Einrichtungen entsprechend berücksichtigen.

2.11.2 Grundlegende Anforderungen zur Gewährleistung der Alltagstauglichkeit

Objekt	**Alltagstauglichkeit**
Schutzbedarfsstufe	**hoch** Begründung: • EPA-Systeme, die aufgrund ihrer Komplexität oder mangelnden Prozessunterstützung, gravierende Schwächen im Hinblick auf Praktikabilität oder Nutzerunterstützung aufweisen, sind eine Quelle für Fehlbedienungen. Daraus kann es zu einer fehlerhaften Verarbeitung von Daten kommen oder zur Aushebelung von Sicherheitsmechanismen.
Kernanforderungen	
Alltag-01	Die Entwicklung eines EPA-Systems sollte strukturiert auf der Basis anerkannter Methoden des Softwareengineerings erfolgen. Grundlegend hierbei ist eine detaillierte Analyse der Behandlungsprozesse mit einrichtungsübergreifender Relevanz und die organisatorischen Gegebenheiten in den medizinischen Einrichtungen.
Alltag-02	Da an ein EPA-System hohe Sicherheitsanforderungen zu stellen sind, ergibt sich u. U. ein Zielkonflikt zwischen Usability und Security. Um dem vorzubeugen sind die Sicherheitsmechanismen, die eine Mitwirkung der Patienten oder der Systembenutzer erfordern, daraufhin zu untersuchen, ob sie sich adäquat in die Geschäftsprozesse integrieren lassen. Eine frühzeitige Festlegung auf bestimmte Technologien sollte vermieden werden. Ein problematischer Sicherheitsmechanismus im Hinblick auf Alltagstauglichkeit ist die patientenzentrierte Verschlüsselung. Dieser Mechanismus dient nicht - wie oft behauptet - primär der Stärkung der Patientenautonomie, sondern ergibt sich aus einer technischen Unzulänglichkeit. Verschlüsselungsverfahren erfordern den Adressaten einer verschlüsselten In-

formation. Dieser steht aber bei einem EPA-System zum Zeitpunkt der Verschlüsselung noch nicht fest, da die künftigen Behandlungssituationen noch unbekannt sind und damit auch die Behandler. Eine EPA dient ja gerade einer asynchronen, einrichtungsübergreifenden Kommunikation. Diese Problematik kann man nun technisch umgehen, indem man den Patienten implizit zum Empfänger macht und ihm das entsprechende kryptographische Schlüsselmaterial an die Hand gibt. Dieser „Trick“ erfordert bis zu einem gewissen Grade eine Patientenmitwirkung bei der Entschlüsselung seiner Daten. Befindet sich das Schlüsselmaterial auf einer Smartcard, muss der Patient sogar körperlich anwesend sein und darüber hinaus auch geistig und körperlich in der Lage sein, zur Freischaltung des Entschlüsselungsprozesses sich gegenüber der Karte zu authentifizieren (also eine PIN in ein Kartenlesegerät einzugeben). Diese Voraussetzungen sind im medizinischen Alltag aber oft nicht gegeben. Einerseits dürften Patienten aufgrund ihres Gesundheitszustandes oder Alters nicht immer in der Lage sein den Authentifizierungsprozess durchzuführen und andererseits gibt es durchaus Situationen, in denen auf EPA-Daten zugegriffen werden muss, der Patient aber körperlich nicht anwesend ist.

2.12 Gewährleistung der Barrierefreiheit

2.12.1 Definition Barrierefreiheit

EPA-Systeme sind so zu konzipieren, dass für alle Betroffenen eine uneingeschränkte Systemteilnahme gegeben ist.

Das Gesundheitswesen wird konfrontiert mit allen Bevölkerungsschichten in allen Altersklassen und eben mit Patienten, also Menschen, die aufgrund ihres Gesundheitszustandes in ihrer Handlungsfähigkeit eingeschränkt sind. Diese Tatsache müssen EPA-Systeme in besonderem Maße berücksichtigen.

Aus Sicht des Datenschutzes bezieht sich die Forderung nach Barrierefreiheit primär auf die Mechanismen zur Durchsetzung der Rechte der Patienten. Das informationelle Selbstbestimmungsrecht garantiert den Patienten bestimmte Rechte, die für den Einzelnen auch faktisch durchsetzbar sein müssen. Darüber hinaus sind weitere spezialgesetzliche Regelungen zu berücksichtigen, wie sie beispielsweise im Gesetz zur Gleichstellung behinderter Menschen zum Ausdruck kommen.

2.12.2 Grundlegende Anforderungen zur Gewährleistung der Barrierefreiheit

Objekt	**Barrierefreiheit**
Schutzbedarfsstufe	**hoch** Begründung: Sieht ein EPA-System keine Mechanismen zur Wahrnehmung der Betroffenenrechte vor, die faktisch von Jedermann ohne Einschränkung nutzbar

	sind, werden die betroffenen Patienten grundlegend in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt. Die Verarbeitung der Daten der Patienten durch ein solches System ist dann durchweg rechtswidrig und zu unterlassen.
Kernanforderungen	
BaFr-01	Aus Sicht des Patienten muss es **eine** verantwortliche Stelle zur Durchsetzung seiner Rechte geben. Diese Stelle berät ihn und setzt seinen Rechtsanspruch faktisch durch.
BaFr-02	Daten, die das EPA-System im Rahmen des Auskunftsrechts bereitstellt, müssen entsprechend patientengerecht aufbereitet sein und den Patienten in analoger Form zur Verfügung gestellt werden können.
BaFr-03	Werden den Patienten technische Zugangsmechanismen (z. B. Kiosksysteme) zur eigenständigen Rechtewahrnehmung zur Verfügung gestellt, wir dadurch die verantwortliche Stelle nicht obsolet. Es kann sich hierbei nur um ein zusätzliches Angebot handeln.
BaFr-04	Das Recht der Patienten auf vertrauliche Behandlung ihrer Daten und deren Nutzungseinschränkung auf das für die jeweilige Behandlung Erforderliche, ist fundamental für ein EPA-System. Die hierzu notwendigen technischen Mechanismen zur patientenzentrierten Verschlüsselung und zur Autorisierung im Behandlungskontext, sind so auszugestalten, dass sie an die Patienten keine höheren Anforderungen stellen, wie es bei analogen Abläufen der Fall ist.