

# **Datenschutz und Telemedizin**

## **- Anforderungen an Medizinnetze -**

Stand 10/02

### Autoren:

Marion Bultmann

Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg

Dr. Rita Wellbrock

Der Hessische Datenschutzbeauftragte

Heinz Biermann

Der Bundesbeauftragte für den Datenschutz

Jürgen Engels

Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

Walter Ernestus

Der Bundesbeauftragte für den Datenschutz

Udo Höhn

Der Bayerische Landesbeauftragte für den Datenschutz

Rüdiger Wehrmann

Der Hessische Datenschutzbeauftragte

Andreas Schurig

Der Sächsische Datenschutzbeauftragte

## **Inhaltsverzeichnis**

I.	Einleitung .....	3
II.	Allgemeine datenschutzrechtliche Anforderungen.....	4
III.	Grundlegende Sicherheitsanforderungen.....	10
IV.	Formen der Datenhaltung .....	14
V.	Spezielle Datensicherheitsmaßnahmen.....	19
VI.	Beispiele für Ansätze/Projekte zur Kommunikation im Gesundheitswesen .....	28

## **I. Einleitung**

Zur Steigerung von Qualität und Effizienz in der Gesundheitsversorgung sowie zur Kosten einsparung spielt die einrichtungsübergreifende elektronische Kommunikation eine immer größere Rolle. Kommunikationsnetze und Kommunikationsdienste sollen dazu beitragen, die Kommunikation zwischen den Institutionen zu verbessern und die Leistungsprozesse zu optimieren. Wegen der hohen Sensibilität der im Gesundheitswesen verarbeiteten Daten kommt dem Datenschutz und der Datensicherheit eine besondere Bedeutung zu.

Die folgenden Ausführungen sollen eine Hilfestellung zur Formulierung und Umsetzung einer datenschutzgerechten Sicherheitspolitik für die elektronische Kommunikation und Datenverarbeitung im Gesundheitswesen bieten. In Kapitel II werden zunächst die allgemeinen datenschutzrechtlichen Anforderungen aufgezeigt. Diese bilden den rechtlichen Rahmen, an dem sich medizinische Datenverarbeitung zu orientieren hat. Darauf aufbauend werden in Kapitel III grundlegende Sicherheitsanforderungen für Systeme definiert, die patientenbezogene Daten verarbeiten. Kapitel IV diskutiert basierend auf der Form der Datenhaltung vier Architekturszenarien für Systeme zur einrichtungsübergreifenden Kommunikation. Damit verbunden ist die Erwartung, dass sich alle Systeme zur einrichtungsübergreifenden Kommunikation nach diesen Architekturansätzen kategorisieren lassen bzw. eine Kombination aus diesen Architekturen darstellen. Insofern sind die zu den Szenarien gemachten Aussagen auf andere Kommunikationsarchitekturen entsprechend übertragbar. In Kapitel V werden für die in Kapitel IV dargestellten Szenarien spezielle Maßnahmen zur Datensicherheit erläutert, die erforderlich sind zur Realisierung der in Kapitel III formulierten Sicherheitsziele und die die hohen Anforderungen an die medizinische Datenverarbeitung berücksichtigen. In Kapitel VI werden schließlich exemplarisch zwei konkrete Ansätze zur Kommunikation im Gesundheitswesen beschrieben.

## **II. Allgemeine datenschutzrechtliche Anforderungen**

Für die Verarbeitung personenbezogener Patientendaten im Rahmen telemedizinischer Anwendungen gelten grundsätzlich die allgemeinen rechtlichen Rahmenbedingungen, die für die Verarbeitung personenbezogener Patientendaten außerhalb telemedizinischer Anwendungen gelten. Die Einführung telemedizinischer Anwendungen darf nicht zu einer rechtlichen oder faktischen Verschlechterung der Patientenrechte führen. Die Durchsetzung bzw. Konkretisierung der Patientenrechte unter den veränderten technischen Bedingungen bedarf teilweise neuer datenschutzrechtlicher Konzepte.

### **Rechtsgrundlagen**

Für die Verarbeitung von Patientendaten durch niedergelassene Ärzte gelten die Vorschriften des BDSG. Für die Verarbeitung von Patientendaten durch die Krankenhäuser gelten in Bund und Ländern unterschiedliche Rechtsvorschriften. In einzelnen Ländern liegen sog. bereichsspezifische Regelungen der Verarbeitung personenbezogener Daten in Krankenhäusern (Landeskrankenhausgesetze, Gesundheitsdatenschutzgesetze etc.) vor. Soweit keine bereichsspezifischen Regelungen vorhanden sind, gelten die allgemeinen datenschutzrechtlichen Vorschriften. Die Religionsgesellschaften treffen für ihren Bereich zum Teil Regelungen in eigener Zuständigkeit. Darüber hinaus sind die Regelungen der Berufsordnung und des Strafgesetzbuchs zu beachten.

Auf der Grundlage des Behandlungsvertrages in Verbindung mit den jeweils maßgeblichen datenschutzrechtlichen Vorschriften darf der Arzt die für die Durchführung der Behandlung erforderlichen Daten verarbeiten. Soweit die Verarbeitung der Daten nicht für die Durchführung der Behandlung erforderlich ist (z.B. zusätzliche Datenerhebungen für ein Forschungsvorhaben), bedarf es einer besonderen Einwilligung des Patienten.

Unabhängig vom verwendeten Datenträger muss der Arzt parallel zu den datenschutzrechtlichen Vorschriften die in der Berufsordnung und in § 203 StGB normierte Schweigepflicht beachten, ferner das in § 5 BDSG und den entsprechenden landesrechtlichen Bestimmungen geregelte Datengeheimnis. Gehilfen des Arztes unterliegen ebenfalls der ärztlichen Schweigepflicht.

## **Dokumentationspflicht**

Nach der Berufsordnung ist der Arzt verpflichtet, die erforderlichen Aufzeichnungen über die in Ausübung seines Berufs gemachten Feststellungen und getroffenen Maßnahmen anzufertigen. Es handelt sich um eine unselbständige vertragliche Nebenpflicht aus dem Behandlungsvertrag. Ist die Dokumentation lückenhaft, kann dies im Haftungsprozess eine Umkehr der Beweislast zugunsten des Patienten nach sich ziehen, wenn die Aufklärung des Sachverhalts für den Patienten insgesamt erschwert wird.

## **Befugnis zur Übermittlung bzw. Weitergabe von Patientendaten**

Der Arzt darf personenbezogene Patientendaten nur im Rahmen der datenschutzrechtlichen Vorschriften und befugt i.S.v. § 203 StGB offenbaren. Eine Befugnis zur Offenbarung kann sich insbesondere aus einer gesetzlichen Regelung (z.B. Krebsregistergesetze, Infektionsschutzgesetz, Sozialgesetzbuch V), aus dem Behandlungsvertrag oder der speziellen Einwilligung des Patienten ergeben. Die ärztliche Schweigepflicht gilt grundsätzlich auch zwischen Ärzten. Eine Übermittlung personenbezogener Daten an einen vor-, mit- oder nachbehandelnden Arzt bedarf daher der Einwilligung des Patienten.

Nach den datenschutzrechtlichen Regelungen müssen Einwilligungen bestimmte Anforderungen erfüllen, um rechtswirksam zu sein. Insbesondere muss die Freiwilligkeit der Einwilligung gewährleistet sein und der Betroffene muss zuvor über Umfang und Zweck der geplanten Verarbeitung seiner Daten, die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung informiert werden (vgl. z.B. § 4a Abs. 1 Satz 1 und 2 BDSG). Pauschale Einwilligungserklärungen, deren Tragweite der Betroffene nicht übersehen kann, sind daher unzulässig. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände im Einzelfall eine andere Form angemessen ist (vgl. z.B. § 4a Abs. 1 Satz 3, Abs. 2 BDSG). Die Landeskrankenhausgesetze enthalten bez. Datenübermittlungen an vor-, mit- und nachbehandelnde Ärzte und an Angehörige zum Teil hiervon abweichende Regelungen (z.B. Widerspruchsrecht des Patienten nach Information über die geplante Datenübermittlung).

Spezialregelungen zur Einwilligung des Versicherten sind insbesondere im SGB V enthalten. Durch das GKV- Gesundheitsreformgesetz 2000 wurden Regelungen zur verstärkten Koope-

ration und Kommunikation zwischen den Leistungserbringern in das SGB V aufgenommen:

- § 73 Abs. I b SGB V enthält eine Spezialregelung zur zentralen Dokumentation beim Hausarzt. Ein Hausarzt darf mit schriftlicher (widerruflicher) Einwilligung des Versicherten bei Leistungserbringern, die einen seiner Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die behandelnden Leistungserbringer sind verpflichtet, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten die Behandlungsdaten und Befunde zum Zwecke der bei diesem durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln; die behandelnden Leistungserbringer sind berechtigt, mit schriftlicher (widerruflicher) Einwilligung des Versicherten, die für die Behandlung erforderlichen Behandlungsdaten und Befunde bei dem Hausarzt und anderen Leistungserbringern zu beschaffen und für die Zwecke der von ihnen zu erbringenden Leistungen zu verarbeiten und zu nutzen.
- In § 140a ff. SGB V sind Regelungen zur sog. integrierten Versorgung enthalten. Die Teilnahme der Versicherten an den integrierten Versorgungsformen ist freiwillig. Die Vertragspartner müssen u.a. die Gewähr dafür übernehmen, dass sie eine an dem Versorgungsbedarf orientierte Zusammenarbeit zwischen allen an der Versorgung Beteiligten sicherstellen, einschließlich der Koordination zwischen den verschiedenen Versorgungsbereichen und einer ausreichenden Dokumentation, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss. Der Leistungserbringer darf aus der gemeinsamen Dokumentation die den Versicherten betreffenden Behandlungsdaten und Befunde nur dann abrufen, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat, die Information für den konkret anstehenden Behandlungsfall genutzt werden soll und der Leistungserbringer zu dem Personenkreis gehört, der nach § 203 StGB zur Geheimhaltung verpflichtet ist.

Das Vorzeigen der Krankenversichertenkarte durch den Patienten beim behandelnden Arzt kann nicht als Einwilligung in die Anforderung bzw. den Abruf von medizinischen Daten bei anderen Ärzten qualifiziert werden, da der Patient in jedem Fall beim behandelnden Arzt seine Krankenversichertenkarte zum Nachweis der Leistungsberechtigung vorlegen muss.

Eine pauschale Einwilligung des Patienten, eine Krankenversichertenkarte mit medizinischen Daten zu verwenden, die bei jedem Arztbesuch vorgezeigt werden muss, ist nach den dargelegten rechtlichen Anforderungen an Einwilligungen unzulässig. Entsprechendes gilt für eine

pauschale Einwilligung des Patienten, dass ein Teil seiner Krankheitsdaten in einem zentralen Datenbestand zum Abruf durch andere Ärzte bereitgehalten werden darf.

## **Informationsrechte des Patienten**

Nach der Rechtsprechung des BGH hat der Patient grundsätzlich ein Recht auf Einsicht in seine Krankenunterlagen, soweit sie sog. objektive Daten betreffen. Es handelt sich um einen Nebenanspruch aus dem Behandlungsvertrag. Für den Bereich der Psychiatrie hat die Rechtsprechung Ausnahmen formuliert. Die – gegenüber der Rechtsprechung vorrangigen - datenschutzrechtlichen Regelungen (Landeskrankenhausgesetze, Gesundheitsdatenschutzgesetze, allgemeine datenschutzrechtliche Regelungen) legen zum Teil weitergehende Rechte der Patienten auf Information, Auskunft und Einsicht fest.

Im Bereich der Telemedizin ist es besonders wichtig, dass der Patient in allen Verarbeitungsphasen ausreichend informiert ist über die Verarbeitung seiner personenbezogenen Daten. Dies setzt voraus, dass das ihn informierende Personal ebenfalls ausreichend informiert ist. Es muss insbesondere auch gewährleistet sein, dass dem Patienten bei Vertragsabschluss bzw. Einwilligung Umfang, Zweck und Rechtsgrundlage der Verarbeitung seiner Daten sowie ggf. die Grundzüge des technischen Verfahrens der Verarbeitung (z.B. bei Chipkartenverfahren) bekannt gegeben worden sind.

## **Datenverarbeitung im Auftrag durch externe Dritte**

In zunehmendem Ausmaß werden personenbezogene medizinische Patientendaten durch externe Dritte verarbeitet. Wenn ein Arzt personenbezogene Patientendaten für eine Auftragsdatenverarbeitung (z. B. Mikroverfilmung, Schreibarbeiten, externe Archivierung) an einen externen Dritten weitergibt, so ist dies keine Datenübermittlung im Sinne der datenschutzrechtlichen Regelungen, da der Arzt als Auftraggeber datenverarbeitende Stelle bleibt. Da die Weitergabe der personenbezogenen Patientendaten an einen externen Dritten jedoch eine Durchbrechung der ärztlichen Schweigepflicht darstellt, benötigt der Arzt für diese Datenweitergabe eine rechtliche Befugnis i.S.v. § 203 StGB. Einige Landeskrankenhausgesetze sehen z. B. die Möglichkeit einer Auftragsdatenverarbeitung für die Krankenhäuser vor. Sofern keine Rechtsvorschrift als Rechtsgrundlage für eine befugte Offenbarung der Patientendaten an

einen externen Dritten vorhanden ist, kommt grundsätzlich nur eine Einwilligung der Betroffenen als Rechtsgrundlage für die Datenweitergabe in Betracht.

Wenn sichergestellt werden kann, dass der externe Dritte (Auftragnehmer) keine personenbezogenen medizinischen Daten zur Kenntnis nehmen kann (z. B. bei Konzepten zur digitalen externen Archivierung, bei denen eine Verschlüsselung aller Informationen vorgesehen ist), liegt keine Durchbrechung der ärztlichen Schweigepflicht vor.

Auch wenn eine Rechtsgrundlage für eine Datenweitergabe zur Auftragsdatenverarbeitung vorliegt, müssen die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit getroffen werden. Dies bedeutet insbesondere auch, dass der Kreis derjenigen Personen, die personenbezogene Patientendaten zur Kenntnis erhalten, soweit wie möglich begrenzt werden bzw. u.U. sogar eine Kenntnisnahme der personenbezogenen Patientendaten ausgeschlossen werden muss.

Die beim Arzt gespeicherten Patientendaten unterliegen dem Beschlagnahmeverbot i. S. v.. § 97 Abs. 1 StPO. Das Beschlagnahmeverbot schützt das Vertrauensverhältnis zwischen dem zeugnisverweigerungsberechtigten Arzt und dem Betroffenen. Das Beschlagnahmeverbot erstreckt sich nur auf Gegenstände, die sich im Gewahrsam des Zeugnisverweigerungsberechtigten befinden. Wenn sich die Patientendaten nicht im Gewahrsam des Zeugnisverweigerungsberechtigten befinden, sondern im Gewahrsam eines externen Dritten, findet das Beschlagnahmeverbot des § 97 StPO keine Anwendung, d.h. der Schutz der Patientenrechte verschlechtert sich. Fraglich ist, ob das Beschlagnahmeverbot ausnahmsweise auch bei Gewahrsam eines externen Dritten Anwendung findet, wenn der externe Dritte (Auftragnehmer) ein Arzt ist. Mangels einer gerichtlichen Entscheidung kann dies nicht als gesichert angesehen werden, denn der Arzt wird hier nicht als behandelnder Arzt tätig, sondern übernimmt eine kommerzielle Tätigkeit.

## **Abruf von Patientendaten über ein Datennetz**

Patientendaten können nach Erteilung einer Einwilligung des Patienten im Einzelfall für einen Zugriff durch den Berechtigten freigegeben werden. Ein Zum – Abruf - Bereitstellen (vgl. z.B. §

10 BDSG) von Patientendaten durch einen Arzt über ein Datennetz ist nach der gegenwärtigen Rechtslage grundsätzlich nicht zulässig. Ein Arzt ist verpflichtet, vor einer Übermittlung zu prüfen, ob eine Befugnis zur Offenbarung der Daten an den Empfänger vorliegt. Würde ein Arzt die Patientendaten für einen Abruf durch andere Behandlungseinrichtungen bereithalten und käme es dann zu einem Abruf, der rechtlich nicht (z. B. durch eine Einwilligung des Patienten) legitimiert ist, so hätte sich der speichernde Arzt nach § 203 StGB strafbar gemacht. Eine Offenbarung von Patientendaten kann auch dadurch vorgenommen werden, dass nicht verhindert wird, dass die Daten durch externe Dritte abgerufen werden können.

### **III. Grundlegende Sicherheitsanforderungen**

Das Bundesdatenschutzgesetz verlangt in § 9 allgemein technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten. Die in der Anlage zu § 9 BDSG beschriebenen Regelungen (die auch denen einiger Länderdatenschutzgesetze entsprechen) definieren Sicherheitsmaßnahmen und haben im Wesentlichen die technischen Komponenten von Datenverarbeitungsanlagen zum Gegenstand. Dadurch sind sie stark technologieabhängig und anpassungs- bzw. erläuterungsbedürftig. Deshalb empfiehlt es sich, sich - wie im Folgenden - zukünftig auf einem abstrakteren Niveau an primär an den Daten ausgerichteten Sicherheitszielen zu orientieren. Dies ist bereits im Rahmen der Novellierung des Datenschutzrechtes in einigen Ländergesetzen geschehen. Sofern andere gesetzliche Regelungen noch den herkömmlichen Katalog der „Zehn Gebote des Datenschutzes“ enthalten, sind diese bei Beachtung der Grundziele und ihrer Umsetzung innerhalb eines Datenschutzkonzeptes in jedem Fall abgedeckt.

Im Folgenden werden die grundlegenden Sicherheitsziele definiert, die von Systemen zur medizinischen Datenverarbeitung gewährleistet werden müssen:

#### **1. Vertraulichkeit**

„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.“ (BVerfGE 32, 373, 380). Die in der ärztlichen Berufsordnung und dem Strafgesetzbuch normierte ärztliche Schweigepflicht schützt das Vertrauensverhältnis zwischen Patient und Arzt. Der Arzt muss die Vertraulichkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten gewährleisten, d.h. nur Befugte dürfen personenbezogene Daten zur Kenntnis erhalten bzw. davon Kenntnis nehmen können. Auch die datenschutzrechtlichen Regelungen, die das Recht des Patienten auf informationelle Selbstbestimmung konkretisieren, schützen die Vertrauensbeziehung zwischen Patient und Arzt. Eine Kenntnisnahme medizinischer Daten durch Unbefugte (z.B. Arbeit-

geber, Versicherungen, Pharmaindustrie) kann erhebliche soziale bzw. materielle Folgen für den Patienten nach sich ziehen.

## **2. Authentizität (Zurechenbarkeit)**

Die Authentizität 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. Ggf. kann auch die Art und Weise der Erhebung der Daten von Bedeutung sein (z.B. Datenerhebung durch ein medizinisches Gerät). Medizinische Dokumente, die ihren Urheber bzw. Verantwortlichen nicht erkennen lassen, sind als Grundlage für Behandlungen und Begutachtungen ungeeignet.

## **3. Integrität**

Die Integrität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, 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. Die Echtheit, Korrektheit und Vollständigkeit der Daten, vor, während und nach der Bearbeitung und Übertragung ist für die Erfüllung des Behandlungsauftrags von großer Bedeutung. Eine Verfälschung oder Unvollständigkeit der Daten kann zu falschen medizinischen Entscheidungen mit u.U. lebensbedrohenden Folgen für den Patienten führen, verbunden mit rechtlichen Konsequenzen für den Mediziner.

## **4. 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.

## **5. 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 festgestellt werden können, wer wann welche patientenbezogenen Daten auf welche Weise verarbeitet hat. Für den Arzt bzw. das Krankenhaus besteht nach der Berufsordnung die Pflicht zur Dokumentation der Behandlung. Sie ist 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 Daten ein Arzt seine Entscheidung über Behandlungsmaßnahmen getroffen hat. Eine notwendige Voraussetzung für die Gewährleistung der Revisionsfähigkeit ist die Sicherstellung der Authentizität.

## **6. Validität**

Die 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. Diese Forderung betrifft insbesondere Bilddaten, bei denen es auf Qualitätsmerkmale wie Bildauflösung und Farbechtheit ankommt. Die Validität wird von der Integrität nicht umfasst, da die Daten zwar integer im Sinne von vollständig und unversehrt sein können, die Darstellungsqualität und Aktualität aber dennoch für medizinische Nutzungszwecke unzureichend sein kann.

## **7. Rechtssicherheit**

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

## **8. Nicht-Abstreitbarkeit von Datenübermittlungen**

Die Nicht-Abstreitbarkeit des Sendens und des Empfangens von patientenbezogenen Dokumenten muss gewährleistet sein. D.h. einerseits ist zu gewährleisten, dass der Sender eines patientenbezogenen Dokuments sicher sein kann, dass das Dokument seinen Empfänger erreicht hat, und er darf nicht abstreiten können, genau dieses Dokument an genau den Empfänger gesendet zu haben. Andererseits muss der Empfänger eines patientenbezogenen Dokuments sicher sein können, genau dieses Dokument von einem bestimmten Sender empfangen zu haben, und er darf nicht abstreiten können, genau das Dokument von einem bestimmten Sender empfangen zu haben. Die Nicht-Abstreitbarkeit ist eine Voraussetzung der Revisionsfähigkeit.

## **9. Nutzungsfestlegung**

Medizinische Datenverarbeitungssysteme müssen es ermöglichen, für jedes patienten-bezogenes Dokument den Nutzerkreis sowie abgestufte Nutzungsrechte festzulegen und Nutzungsausschlüsse zu definieren.

## **IV. Formen der Datenhaltung**

In diesem Kapitel werden Systeme zur einrichtungsübergreifenden Verarbeitung patientenbezogener Daten in Kategorien unterteilt, die in den folgenden Szenarien beschrieben werden. Die Kriterien für die Kategorisierung orientieren sich an den grundlegenden Formen der Datenhaltung. Es ist zu erwarten, dass jedes medizinische Datenverarbeitungssystem zur einrichtungsübergreifenden Kommunikation einer dieser Kategorien angehört oder sich als eine Kombination dieser darstellt. Damit wird es möglich Systeme einzurichten und die zu den einzelnen Szenarien getroffenen Aussagen entsprechend auf das jeweils zu betrachtende System zu übertragen.

### **Szenario 1: Dezentrale Datenhaltung:**

Bei der dezentralen Datenhaltung werden die Daten dort gespeichert, wo sie auch erzeugt wurden. Somit hat jede medizinische Einrichtung ihre eigene Datenhaltung. Die Datenhaltungssysteme der verschiedenen Einrichtungen können zwar über ein Netz miteinander kommunizieren, sind aber ansonsten als vollständig autonom anzusehen. Systemübergreifende einheitliche Dienste gibt es nicht.

Bei einer dezentralen Architektur muss für jeden Kommunikationsvorgang explizit eine Kommunikationsverbindung zwischen dem sendenden und dem empfangenden System aufgebaut werden. Die Initiierung der Kommunikation erfolgt durch den Sender. Dies erfordert, dass vor jeder Übermittlung von Dokumenten eines Patienten dem Sender (z.B. dem überweisenden Arzt) der Empfänger (z.B. der weiterbehandelnde Arzt) bekannt sein muss. Eine nicht-adressierte Kommunikation ist nicht möglich. Die Realisierung einer einrichtungsübergreifenden elektronischen Patientenakte ist daher nicht bzw. nur sehr eingeschränkt möglich (z.B. fallbezogen durch jeweiliges Mitsenden der bereits vorhandenen Dokumente).

Jede Einrichtung ist datenverarbeitende Stelle i.S. der Datenschutzgesetze für ihre eigenen Daten. Datenübermittlungen an vor-, mit- und nachbehandelnde Ärzte sind nur aufgrund einer rechtlichen Legitimation (z.B. Einwilligung des Patienten im Einzelfall) zulässig. Spezielle rechtliche oder rechtspolitische Probleme bzgl. der ärztlichen Schweigepflicht entstehen bei der dezentralen Datenhaltung nicht.

## **Szenario 2: Zentrale Datenhaltung:**

Bei der zentralen Datenhaltung werden Daten, deren Verarbeitung in der Verantwortung verschiedener medizinischer Einrichtungen liegt, (technisch) zentral zusammengeführt und in einem zentralen System gespeichert. Es gibt keine redundanten Datenbestände, d.h. bei den verschiedenen beteiligten Einrichtungen selbst werden keine Daten gespeichert.

Die Einrichtungen bleiben jeweils datenverarbeitende Stelle i.S. der Datenschutzgesetze für ihre eigenen Datenbestände. Eine einrichtungsübergreifende zentrale Datenhaltung kann nur über die Vergabe einer Datenverarbeitung im Auftrag an einen externen Dritten realisiert werden. Die rechtlichen Voraussetzungen für eine Datenverarbeitung im Auftrag müssen erfüllt sein (s. Kapitel II). Auch wenn die rechtlichen Voraussetzungen erfüllt sind, bleibt es problematisch, dass der Beschlagnahmeschutz für die Patientendaten durch die Auftragsdatenverarbeitung aufgehoben ist und dass Dritte Kenntnis der medizinischen Daten erhalten. In jedem Fall muss die Möglichkeit der Kenntnisnahme personenbezogener medizinischer Daten durch den externen Dritten soweit wie möglich ausgeschlossen werden.

Im übrigen ist die ärztliche Schweigepflicht gewahrt, wenn der Zugriffskontrollmechanismus des Zentralsystems gewährleistet, dass jede Einrichtung nur auf die eigenen Daten zugreifen kann.

Datenübermittlungen zwischen den angeschlossenen Einrichtungen werden technisch durch entsprechende Rechtevergaben realisiert. Will ein Mediziner der Einrichtung A ein Dokument X an einen Mediziner der Einrichtung B übermitteln, veranlasst er, dass dieser die Zugriffsrechte für dieses Dokument erhält.

Wie bei Szenario 1 muss eine rechtliche Legitimation für die Datenübermittlungen vorliegen. Der Patient kann einwilligen, dass seine Daten einem bestimmten Arzt übermittelt werden. Es ist auch möglich, dass der Patient darin einwilligt, dass ein Teil seiner Daten zum Abruf durch einen später von ihm bestimmten Arzt bereitgehalten werden. Die Voraussetzungen, unter denen ein Arzt auf die Daten zugreifen darf, müssen in der Einwilligungserklärung festgelegt sein. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Zugriff durch den jeweiligen Arzt vorliegen.

Mit diesem Modell ist die elektronische Patientenakte sowohl fallbezogen als auch umfassend realisierbar, soweit die einen Patienten behandelnden Einrichtungen bzw. Ärzte sich an der zentralen Datenhaltung beteiligen und die Einwilligung des Patienten vorliegt.

Unter rechtspolitischen Gesichtspunkten ist die zentrale Datenhaltung problematisch, weil eine zentrale Datensammlung über Patienten neue Missbrauchsmöglichkeiten eröffnet und neue Begehrlichkeiten nach weiteren zentralen Auswertungs- und Verwendungsmöglichkeiten der Patientendaten wecken kann.

### **Szenario 3: Verteilte Datenhaltung**

Bei der verteilten Datenhaltung werden, wie im Falle der dezentralen Datenhaltung, die Daten auf den Systemen der Einrichtungen gespeichert, die sie auch erzeugt haben. Darüber hinaus gibt es aber systemübergreifende Dienste, die dafür sorgen, dass die einzelnen dezentralen Systeme zu einem Kommunikationsverbund zusammengeschlossen werden. Damit sind die dezentralen Systeme Subsysteme des durch den Verbund entstandenen Gesamtsystems. Den Nutzern eines verteilten Systems bleibt die physikalische Verteilung der Daten auf eine Vielzahl von Subsystemen verborgen (Verteilungstransparenz) und ihnen wird der Eindruck vermittelt, als arbeiten sie mit einem Zentralsystem. Ein verteiltes System benötigt Metainformationen über die bei den einzelnen Subsystemen gespeicherten Dokumente sowie einen systemweiten Zugriffskontrollmechanismus.

Die Einrichtungen bleiben jeweils datenverarbeitende Stelle i.S. der Datenschutzgesetze für ihre eigenen Datenbestände. Datenübermittlungen zwischen den verschiedenen Einrichtungen, d.h. zwischen dezentralen Subsystemen, erfordern wie bei der zentralen Datenhaltung eine rechtliche Legitimation und eine entsprechende Rechtevergabe. Möchte ein Mediziner der Einrichtung A (Nutzer des Subsystems A) auf ein Dokument zugreifen, prüft der systemweite Zugriffskontrollmechanismus, ob er die entsprechenden Zugriffsrechte besitzt. Ist dies der Fall, ermittelt ein Systemdienst auf der Grundlage der Metainformationen den Lagerort des Dokumentes. Ist das Dokument bei Subsystem A gespeichert (also ein Dokument der Einrichtung A), erfolgt ein lokaler Datenzugriff. Ist das Dokument bei Subsystem B gespeichert (also ein Dokument der Einrichtung B), erfolgt ein entfernter Zugriff auf Subsystem B unter

Nutzung von Kommunikationsmechanismen, ohne dass der Nutzer Kenntnis des Speicherortes haben muss.

Bei der verteilten Datenhaltung bleiben die verschiedenen Einrichtungen datenverarbeitende Stelle i.S. der Datenschutzgesetze für ihre eigenen Daten. Grundsätzlich ist die ärztliche Schweigepflicht gewahrt, wenn jede Einrichtung nur auf ihre eigenen Daten zugreifen kann.

Der Patient kann einwilligen, dass seine Daten an einen bestimmten Arzt übermittelt werden. Es ist auch möglich, dass ein Teil seiner Daten für externe Zugriffe durch später von ihm bestimmte Ärzte unter den von ihm bestimmten Voraussetzungen bereitgehalten werden. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Datenzugriff durch den jeweiligen Arzt vorliegen. Der Aufbau einer einrichtungsübergreifenden („virtuellen“) elektronischen Patientenakte ist bei diesem Modell möglich.

Bei der verteilten Datenhaltung wird das o.a. rechtspolitische Problem der zentralen Datenhaltung gemildert, da selbst im „worst case“ nur die Daten zusammengeführt werden können, die für externe Zugriffe freigegeben wurden. Der Beschlagnahmeschutz für die Patientendaten bleibt erhalten. Da die verteilte Datenhaltung keine Datenverarbeitung im Auftrag erforderlich macht, ist das Problem der Kenntnisnahme von personenbezogenen medizinischen Patientendaten durch externe Dritte nicht gegeben.

#### **Szenario 4: Dezentrale Datenhaltung mit zentraler Komponente**

Bei dieser Datenhaltungsform findet eine dezentrale Datenhaltung bei den einzelnen medizinischen Einrichtungen statt. Außerdem können Dokumente der verschiedenen Einrichtungen an einer zentralen Stelle temporär (technisch) zusammengeführt werden.

Die verschiedenen Einrichtungen bleiben datenverarbeitende Stelle i.S. der Datenschutz-gesetze für ihre eigenen Daten, auch bei der zentralen Speicherung eines Teildatenbestandes.

Bei diesem Modell bildet die zentrale Speicherkomponente einen Puffer, der allen ange-schlossenen Einrichtungen zum Up- und Download zur Verfügung steht. Dokumente werden vom Sender auf diesen zentralen Speicher übertragen (Upload) und können dann vom Empfänger von dort abgeholt (Download) werden.

Rechtlich handelt es sich beim Up- und dem zugehörigen Download um eine Datenübermittlung, die einer rechtlichen Legitimation (z.B. Einwilligung des Patienten) bedarf. Der Patient kann im Einzelfall einwilligen, dass seine Daten einem bestimmten Arzt über die zentrale Speicherkomponente übermittelt werden. Es ist auch möglich, dass der Patient darin einwilligt, dass ein Teil seiner Krankheitsdaten in den zentralen Datenbestand eingestellt wird und dort zum Abruf durch später von ihm bestimmte Ärzte bereitgehalten wird. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Abruf der Daten durch den jeweiligen Arzt vorliegen. Auf dem zentralen Speicher können Dokumente zur (fallbezogenen) elektronischen Patientenakte zusammengeführt werden, soweit der den Patienten behandelnde Arzt an die zentrale Speicherkomponente angeschlossen ist und eine Einwilligung des Patienten in die Bereitstellung der Daten für den Abruf durch andere Ärzte vorliegt.

Die zentrale einrichtungsübergreifende Speicherung eines Teildatenbestandes aller Einrichtungen kann nur über die Vergabe einer Datenverarbeitung im Auftrag an einen externen Dritten realisiert werden. Die rechtlichen Voraussetzungen für eine Datenverarbeitung im Auftrag müssen erfüllt sein. Auch wenn die rechtlichen Voraussetzungen erfüllt sind, bleibt es problematisch, dass der Beschlagnahmeschutz für die Patientendaten durch die Auftragsdatenverarbeitung aufgehoben ist. Die Möglichkeiten einer Kenntnisnahme personenbezogener medizinischer Daten durch den externen Dritten müssen in jedem Fall soweit wie möglich ausgeschlossen werden.

Bei der dezentralen Datenhaltung mit zentraler Komponente entsteht das auch bei der zentralen Datenhaltung dargelegte rechtspolitische Problem: Es entsteht eine neue zentrale (Teil-)Datensammlung, die neue Möglichkeiten des Datenmissbrauchs eröffnet und neue Begehrlichkeiten nach weiteren zentralen Datenauswertungen und –verwendungen wecken kann.

## **V. Spezielle Datensicherheitsmaßnahmen**

Zur Realisierung der in Kapitel III definierten Sicherheitsziele sind für jedes medizinische Datenverarbeitungssystem auf der Grundlage einer Bedrohungs- und Risikoanalyse die individuell erforderlichen Sicherheitsmaßnahmen zu ermitteln. Naturgemäß ergibt sich eine Vielzahl zu treffender technischer und organisatorischer Sicherheitsmaßnahmen, die abhängig von den jeweiligen technischen Systemausprägungen und den unterschiedlichen Rahmenbedingungen von System zu System sehr unterschiedlich sein können. Aufgrund des hohen Schutzbedarfs der Daten, die von medizinischen Systemen verarbeitet werden, ergeben sich aber spezielle Sicherheitsmaßnahmen, die aus datenschutzrechtlicher Sicht als unabdingbar anzusehen sind. Diese Maßnahmen werden im Folgenden für die einzelnen Sicherheitsziele und Systemarchitekturen erläutert.

### **1. Sicherstellung der Vertraulichkeit**

Der Vertraulichkeit kommt aufgrund der hohen Sensibilität medizinischer Daten und der Pflicht zur Wahrung des Arzt-Patienten-Geheimnisses eine große Bedeutung zu. Insofern muss bei jeder Phase der Datenverarbeitung sichergestellt werden, dass nur Befugte patientenbezogene Daten zur Kenntnis nehmen können. Eine hinreichende Gewährleistung der Vertraulichkeit mit den hohen Anforderungen des Gesundheitswesens kann nur durch Verschlüsselung der patientenbezogenen Daten mit starken kryptografischen Verfahren erreicht werden. Zum einen ist eine Verschlüsselung aller Daten zu fordern, die über ein Kommunikationsnetz übertragen werden und zwar unabhängig davon, ob es sich um ein lokales oder um ein öffentliches Netz handelt. Daneben sind alle bei den datenhaltenden Systemen gespeicherten Daten zu verschlüsseln. Nur so kann verhindert werden, dass Systemadministratoren, Wartungspersonal oder sonstige Dritte (z.B. durch Diebstahl) Kenntnis von Daten erhalten, die dem Arzt-Patienten-Geheimnis unterliegen.

### **(a) Verschlüsselung übertragener Daten:**

Die Übertragung patientenbezogener Daten in dezentralen Systemen erfordert eine Verschlüsselung auf Anwendungsebene. Da die Systeme in dezentralen Architekturen autonom sind und sich somit aus der Sicht eines Systems die übrigen Systeme jeweils wie Black Boxes darstellen, kann nur die an Personen adressierte Verschlüsselung sicherstellen, dass nur Befugte die übermittelten Daten zur Kenntnis nehmen können.

In zentralen Systemen reicht eine Verschlüsselung auf Transportebene aus, da alle Nutzer dem Zugangs- und Zugriffskontrollmechanismus des Systems unterliegen.

In einem verteilten System reicht ebenso eine Verschlüsselung auf Transportebene aus, wenn es für den systemübergreifenden Datenaustausch einen einheitlichen, systemweiten Zugangs- und Zugriffskontrollmechanismus gibt.

Die dezentrale Architektur mit zentraler Komponente kann im Prinzip gehandhabt werden wie eine dezentrale Architektur, da die zentrale Komponente die Funktion eines „Postfaches“ übernimmt, aus dem sich der Empfänger seine Nachricht abholt.

### **(b) Verschlüsselung gespeicherter Daten:**

Die verschlüsselte Speicherung der Daten bei den datenhaltenden Systemen kann realisiert werden durch den Einsatz entsprechender Systemsoftware (z.B. Datenbanksysteme, die eine Datenverschlüsselung ermöglichen) oder durch entsprechende Zusatzsoftware (z.B. Tools zur Verschlüsselung von Plattenbereichen). Eine andere Möglichkeit zur Lösung dieses Problems besteht in der Verschlüsselung der patientenbezogenen Dokumente auf Anwendungsebene. Dabei bietet sich eine Hybridverschlüsselung an, wobei das Dokument selbst mit einem symmetrischen Schlüssel (Session Key) verschlüsselt wird und der symmetrische Schlüssel jeweils mehrfach nach einem asymmetrischen Verfahren mit den öffentlichen Schlüsseln der berechtigten Nutzern. Der für ein Dokument verantwortliche Mediziner legt dann (u.U. unter Mitwirkung des Patienten) bei der Aktivierung des Verschlüsselungsvorgangs die berechtigten Personen fest. Diese Vorgehensweise stellt sicher, dass nur berechtigte Nutzer in die Lage versetzt werden, ein Dokument zu entschlüsseln und realisiert damit gleichzeitig einen

Zugriffskontrollmechanismus (bezogen auf Lesevorgänge). Das Verschlüsselungskonzept muss ein Verfahren vorsehen, dass eine Verfügbarmachung der Daten im Notfall gewährleistet.

## **2. Gewährleistung der Authentizität**

Patientenbezogene Dokumente sind von ihrem Urheber bzw. von dem verantwortlichen Mediziner elektronisch zu signieren und mit einem Zeitstempel zu versehen. Nur durch die elektronische Signatur kann die Zurechenbarkeit von Dokumenten zum Urheber bzw. zum Verantwortlichen sichergestellt werden.

Die erforderlichen Mechanismen zur elektronischen Signatur von Dokumenten sind unabhängig von der gewählten Architektur der Datenhaltung.

## **3. Sicherstellung der Integrität**

Mit dem elektronischen Signieren eines patientenbezogenen Dokumentes zur Sicherstellung der Authentizität wird gleichzeitig die Echtheit, Korrektheit und Vollständigkeit des Dokumenteninhalts bescheinigt, da der Signaturvorgang eine bewusste Handlung vom Signierenden erfordert. Der Mediziner, der ein Dokument elektronisch signiert, also sozusagen elektronisch unterschreibt, bestätigt mit seiner Signatur nicht nur, dass er der Urheber bzw. der Verantwortliche ist, sondern gleichzeitig, dass das Dokument echt sowie inhaltlich korrekt und vollständig ist. Darüber hinaus sichert das der elektronischen Signatur zugrunde liegende kryptografische Verfahren die Erkennbarkeit einer nachträglichen Veränderung eines Dokuments. Die erfolgreiche Verifikation der Signatur eines Dokuments stellt damit gleichzeitig die Unversehrtheit des Dokumenteninhalts sicher.

## **4. Sicherstellung der Verfügbarkeit**

Bei der Sicherstellung der Verfügbarkeit, teilen sich die verschiedenen Architekturansätze in zwei Lager:

- (1) Sowohl im Falle der zentralen Datenhaltung als auch im Falle der dezentralen Datenhaltung mit zentraler Komponente ist eine hohe Verfügbarkeit realisierbar. Da bei der zentralen Datenhaltung ausschließlich die zentrale Datenverarbeitungsanlage Daten speichert und verarbeitet, sind die technischen Möglichkeiten gegeben für diese Anlage und damit für das gesamte System eine Hochverfügbarkeit zu gewährleisten. Die Situation bei der dezentralen Datenhaltung mit zentraler Komponente ist vergleichbar. Die für den einrichtungsübergreifenden Datenaustausch vorgesehenen Daten werden von der zentralen Komponente gespeichert, für die ebenso eine Hochverfügbarkeit realisierbar ist. Einschränkungen der Verfügbarkeit des Gesamtsystems können sich nur ergeben aus einer temporären Nichtverfügbarkeit von angeschlossenen dezentralen Systemen für einen notwendigen Upload oder Download.
- (2) Bei der dezentralen und verteilten Datenhaltung hängt die Verfügbarkeit des Gesamtsystems von der Verfügbarkeit aller beteiligten (Sub-)Systeme ab. Bei der dezentralen Datenhaltung müssen die datenhaltenden Systeme als autonom angesehen werden, was einer systemweiten Verfügbarkeitsregelung entgegensteht. Insbesondere im niedergelassenen Bereich dürften sich die Verfügbarkeitszeiten der Systeme auf die Praxiszeiten beschränken, die zudem von Praxis zu Praxis noch unterschiedlich sein können. Insofern ist schon aus organisatorischen Gründen eine hohe Verfügbarkeit des Gesamtsystems nicht realisierbar. Bei der verteilten Datenhaltung müssen Kommunikationsprozesse – im Gegensatz zum dezentralen Fall- nicht explizit von den Nutzern eines Subsystems initiiert werden, sondern können durch systemweit verfügbare Kommunikationsmechanismen angestoßen werden. Insofern wird die Verfügbarkeit nicht notwendigerweise von beschränkten Praxiszeiten determiniert. Allerdings kann es zu technisch bedingten Ausfällen von Subsystemen kommen, die ohne Eingriffe vor Ort nicht behebbar sind. Solchen Schwierigkeiten kann man technisch dadurch begegnen, dass Datenreplikate an verschiedenen Speicherorten vorgehalten werden. Bei Nichtverfügbarkeit eines bestimmten Subsystems wird dann auf das entsprechende Replikat zurückgegriffen. Diese Vorgehensweise ist allerdings datenschutzrechtlich als sehr problematisch einzustufen, wenn die Replikate sich nicht im selben Herrschaftsbereich befinden, wie ihre Originale. Außerdem ergeben sich durch Replikate nicht zu unterschätzende Konsistenzprobleme. Letztlich ist auch im verteilten Fall die Verfügbarkeit

abhängig von der Verfügbarkeit der beteiligten Subsysteme. Eine Hochverfügbarkeit dürfte nicht oder nur mit sehr hohen Aufwand realisierbar sein.

## **5. Gewährleistung der Revisionsfähigkeit**

Grundvoraussetzung für die Gewährleistung der Revisionsfähigkeit ist das elektronische Signieren der patientenbezogenen Dokumente, weil hiermit die Verantwortlichkeit bzw. Urheberschaft anerkannt wird. Da der Inhalt eines signierten Dokuments nachträglich nicht mehr verändert werden kann, ohne die Signatur zu verletzen, können inhaltliche Änderungen nur in Form von Ergänzungen einem Dokument angefügt werden. Wird das Ursprungsdocument plus Ergänzungen wiederum digital signiert, kann die Historie eines Dokuments manipulationssicher festgehalten werden.

Die von der Dokumentensignatur nicht erfassbaren Verarbeitungsschritte des Übermitteln eines Dokuments und des Lesen eines Dokuments sind mittels einer manipulationssicheren Protokollierung einer Revision zugänglich zu machen. Das vollständige Löschen eines Dokuments muss aus Gründen der Dokumentationspflicht in jedem Fall vom Zugriffskontrollmechanismus unterbunden werden.

Eine Protokollierung ist bei zentralen Systemen naturgemäß recht einfach und umfassend zu realisieren, da hierbei die Datenverarbeitung von nur einem System vorgenommen wird, welches damit auch die Kontrolle über alle Verarbeitungsphasen eines Dokuments hat und außerdem die einzelnen Verarbeitungsschritte den Personen zuordnen kann, die sie verursacht haben.

Hingegen durchläuft ein Dokument im Zuge seiner Verarbeitung bei einem dezentralen System u.U. mehrere lokale Systeme. Da es in einem dezentralen System keine zentrale Kontrollinstanz über die Verarbeitungsschritte der Einzelsysteme gibt, ist eine zentrale Protokollierung nicht möglich. Hier bleibt nur die Protokollierung durch die lokalen Systeme.

Die Protokollierung von Lesevorgängen ist problemlos möglich. Die Protokollierung von Übermittlungsvorgängen erfordert allerdings die Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangs von Dokumenten. Für die Revision der Gesamtheit aller Verarbeitungsschritte eines Dokuments ist allerdings das Zusammenführen der relevanten Protokolldaten aller lokaler Systeme erforderlich, die das Dokument durchlaufen hat.

Bei verteilten Systemen können systemweit zur Verfügung stehende Dienste zur Protokollierung von Verarbeitungsschritten genutzt werden, die systemübergreifende Wirkung haben (also im Wesentlichen Datenübermittlungen). Alle anderen Aktivitäten, die nicht von systemweiten Diensten abhängen, können wie in dezentralen Systemen nur von den beteiligten lokalen Subsystemen protokolliert werden.

Die dezentrale Datenhaltung mit zentraler Komponente erlaubt eine Protokollierung aller Aktivitäten, die sich auf die zentrale Komponente beziehen, wie die zentrale Datenhaltung. Alle Aktivitäten, die sich auf die lokalen Systeme beschränken, müssen von diesen protokolliert werden. Die Protokollierung von Datenübermittlungen zwischen den lokalen Systemen und der zentralen Komponente erfordert wiederum die Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangs von Dokumenten.

## **6. Gewährleistung der Validität**

Die Sicherstellung der Validität ist prinzipiell unabhängig von der Architektur der beteiligten Systeme. Sie ist aber in hohem Maße abhängig von einer Standardisierung der für die Validität relevanten Systemkomponenten (Hard- und Softwarekomponenten). Insofern ist anzunehmen, dass eine valide Datenverarbeitung umso schwieriger herstellbar ist, je heterogener die zu betrachtende Systemlandschaft ist.

## **7. Gewährleistung der Rechtssicherheit**

Die Voraussetzung für die Rechtsicherheit ist die Revisionsfähigkeit und damit auch das elektronische Signieren eines jeden patientenbezogenen Dokuments. Damit eine elektronische Signatur rechtsverbindlich einer verantwortlichen Person zugeordnet werden kann, bedarf es der qualifizierten Signatur. Erst die qualifizierte Signatur gewährleistet eine rechtswirksame Überprüfbarkeit der Zuordnung einer Signatur zu der Person, die die Signatur erzeugt hat.

## **8. Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen**

Die Nichtabstreitbarkeit des Sendens und Empfangs spielt primär eine Rolle in Architekturen mit dezentraler Ausrichtung, da aufgrund der Autonomie der lokalen Systeme eine Daten-

übermittlung explizit von einem Systemnutzer angestoßen werden muss und es keine systemübergreifenden Kontrollmechanismen gibt, die einen Übermittlungsvorgang technisch überwachen und im Fehlerfall entsprechende Maßnahmen einleiten.

Die Nicht-Abstreitbarkeit in einem dezentralen System ist nur über ein Quittungsverfahren unter Verwendung elektronischer Signaturen zu realisieren. Der Sender eines Dokuments versieht dieses zunächst mit einer elektronischen Signatur und sendet es an den Empfänger. Der Empfänger verifiziert die Signatur, um festzustellen, ob das Dokument von dem angegebenen Sender stammt. Dann muss der Empfänger dem Sender bestätigen, dass er ein Dokument mit bestimmten Inhalt von ihm bekommen hat. Diese Empfangsbestätigung kann realisiert werden, indem von dem empfangenen Dokument der Hashwert gebildet wird und dieser zusammen mit einem das Dokument identifizierenden Merkmal (und evtl. mit der Eingangszeit) vom Empfänger elektronisch signiert an den Sender gesendet wird. Der Sender verifiziert die Signatur der Quittung, bildet seinerseits den Hashwert des von ihm gesendeten Dokuments und vergleicht diesen mit dem in der Quittung zugesandten Hashwert. Stimmen beide Werte überein, kann der Sender sicher sein, dass genau der von ihm spezifizierte Empfänger (aufgrund der Signaturverifikation) auch genau das von ihm gesendete Dokument (aufgrund des Vergleichs der Hashwerte) erhalten hat. Schlägt die Signaturverifikation oder der Hashwertvergleich fehl, muss sich der Sender mit dem Empfänger in Verbindung setzen. Erhält der Empfänger keine Reklamation durch den Sender, dann kann er seinerseits sicher sein, dass das empfangene Dokument genau von dem vermuteten Sender kommt, mit genau dem vom Sender gesendeten Inhalt. Erhält bei diesem Quittungsverfahren der Sender nach einer gewissen Zeit keine Quittung für seine gesendete Nachricht, so ist entweder die Nachricht oder die Quittung nicht zugestellt worden. Für diesen Fall ist eine adäquate Handlungsweise zu vereinbaren (z.B. erneutes Senden der Nachricht nach einer Wartefrist oder Kontaktieren des Empfängers).

Solch ein Quittungsverfahren ist natürlich softwaretechnisch entsprechend so zu unterstützen, dass es so weit wie möglich automatisiert abläuft. Ein Standard-Email-System ist nicht in der Lage, die Forderung der Nicht-Abstreitbarkeit zu erfüllen.

Bei einem dezentralen System mit zentraler Komponente ist ein solches Quittungsverfahren in modifizierter Form ebenfalls realisierbar. Hier erhält der Sender einer Nachricht eine Quittung von der zentralen Komponente und der Empfänger sendet seine Quittung an die zentrale Komponente. Die Nicht-Abstreitbarkeit ist dann über die Informationskette Sender, Protokolldaten der zentralen Komponente, Empfänger herstellbar.

Die Signatur von Dokumenten zur Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen ist nicht zu verwechseln mit der Signatur von Dokumenten zur Gewährleistung der Authentizität. Im ersten Fall dient die Signatur der Zuordnung eines Dokuments zu seinem Sender, im zweiten Fall der Zuordnung eines Dokuments zu seinem Urheber. Da der Sender eines Dokuments aber nicht notwendigerweise auch der Urheber ist, muss jedes Dokument bei einer Übermittlung vom Sender elektronisch signiert werden.

Bei zentralen und verteilten Architekturen ist die Nicht-Abstreitbarkeit auf der Grundlage der entsprechenden Protokollinformationen realisierbar.

## **9. Gewährleistung der Nutzungsfestlegung**

Da im zentralen Fall der Zugriffskontrollmechanismus eine systemweite Kontrolle ausüben kann, ist eine Nutzungsfestlegung prinzipiell umfassend zu realisieren. Es kommt nur darauf an welche Differenzierung das Berechtigungskonzept bzw. die Zugriffskontrolle des jeweiligen Systems zulässt. Aufwendig könnte die Umsetzung eines Nutzungsausschlusses sein (z.B. leseberechtigt sind alle Mediziner der Abteilung A (Rolle) mit Ausnahme von Herrn Dr. X der Abteilung A).

Existiert in einem System mit verteilter Datenhaltung ein systemweites Berechtigungskonzept und ein systemweiter Zugriffskontrollmechanismus sind Nutzungsrechte, die systemübergreifende Bedeutung haben, wie bei einem Zentralsystem definierbar.

Bei dezentralen Systemen sind Nutzungsrechte mittels des Zugriffskontrollmechanismus jeweils für die lokalen Systeme definierbar. Wird ein Dokument von einem lokalen System an ein anderes übermittelt, müssen die u.U. bestehenden Nutzungsrechte bzw. Nutzungsausschlüsse mit dem Dokument übermittelt werden. Der Empfänger des Dokuments muss dann für deren Einhaltung sorgen.

Dezentrale Systeme mit zentraler Komponente können Zugriffskontrollmechanismen für die zentrale Komponente wie im zentralen Fall realisieren. Dokumente, die sich im Speicherbereich der Subsysteme befinden oder in deren Speicherbereich gelangen, entziehen sich dem zentralen Zugriffskontrollmechanismus und sind wie im dezentralen Fall zu behandeln.



## **VI. Beispiele für Ansätze/Projekte zur Kommunikation im Gesundheitswesen**

### **1. Patientenbegleitende Dokumentation (PaDok)**

PaDok wurde vom Fraunhofer-Institut für Biomedizinische Technik als technische Lösung zur Erfüllung eines großen Teils der alltäglichen Kommunikation von Leistungserbringern im Gesundheitswesen entwickelt. Technisch realisiert sind zur Zeit der elektronische Arztbrief, die elektronische Überweisung, die elektronische Einweisung, die elektronische Quartalsabrechnung, das elektronische Rezept und die elektronische Fall-Akte. Von seiner Architektur unterstützt PaDok eine dezentrale Datenhaltung mit zentraler Komponente. Die zentrale Komponente wird von einem PaDok-Server gebildet, der als Nachrichtenpuffer dient. Der Absender einer Nachricht versieht eine elektronische Information mit einer Empfänger-Kennung und schickt sie an den PaDok-Server, der an einer zentralen Stelle im regionalen Netzwerk steht. Der Empfänger der Nachricht kann sich dann die Nachricht vom PaDok-Server abholen. Insofern gleicht das Grundprinzip von PaDok dem der E-Mail. Alle PaDok-Nachrichten werden elektronisch signiert und mittels eines asymmetrischen Verfahrens verschlüsselt. Damit ist die Vertraulichkeit, Integrität und Authentizität von PaDok-Nachrichten sichergestellt.

Im Gegensatz zu einem Standard-Mailingsystem erlaubt PaDok die nicht-adressierte Kommunikation. Wird beispielsweise ein Patient von seinem Hausarzt zwecks einer internistischen Weiterbehandlung überwiesen, steht u.U. zum Zeitpunkt der Überweisung der Internist als Person noch nicht fest, da der Patient die freie Arztwahl hat. Das Problem besteht nun darin, dass zum Verschlüsseln der zu übermittelnden Dokumente mittels eines asymmetrischen Verfahrens der öffentliche Schlüssel des Empfängers erforderlich ist, also zum Zeitpunkt der Verschlüsselung der konkrete Empfänger feststehen muss. PaDok löst dieses Problem, indem es die Dokumente des Absenders (hier der Hausarzt), die an den Empfänger (hier der noch nicht feststehende Internist) übermittelt werden sollen, mit einer Vorgangskennung versieht. Diese Vorgangskennung besteht aus zwei Teilen. Der eine Teil dient der Identifikation der Dokumente und der andere Teil wird als Schlüssel (Vorgangsschlüssel) verwendet. Vereinfacht ausgedrückt werden nun die Dokumente durch ein zweistufiges Verschlüsselungsverfahren verschlüsselt. Dazu ist der Vorgangsschlüssel und der öffentliche Schlüssel des PaDok-Servers erforderlich. Die verschlüsselten Dokumenten werden an den PaDok-Server versandt und der Patient erhält die Vorgangskennung, entweder in ausgedruckter Form oder auf einer Chipkarte. Findet sich der Patient schließlich bei einem weiterbehandelnden Internisten seines Vertrauens ein, so übergibt

er ihm die Vorgangskennung. Der identifizierende Teil der Vorgangskennung dient nun der Selektion der Dokumente auf dem PaDok-Server. Der PaDok-Server entschlüsselt die selektierten Dokumente mit dem geheimen Server-Schlüssel und verschlüsselt sie anschließend mit dem öffentlichen Schlüssel des anfordernden Internisten. Die Verschlüsselung, die mit dem Vorgangsschlüssel erfolgte, bleibt bei diesem Umschlüsselungsvorgang erhalten, so dass die Dokumente auf dem Server zu keinem Zeitpunkt lesbar sind. Die umgeschlüsselten Dokumente werden dann an den Internisten geschickt. Dieser benötigt zur Entschlüsselung seinen geheimen Schlüssel und den in der Vorgangskennung enthaltenen Vorgangsschlüssel. Mit diesem Verfahren ermöglicht PaDok eine nicht-adressierte Kommunikation unter Wahrung einer adressierten Vertraulichkeit. Der Patient wird dadurch in die Lage versetzt, den Adressaten seiner Dokumente (hier der weiterbehandelnde Internist) selbst zu bestimmen, ohne dass er diesen dem Absender der Dokumente (hier der überweisende Hausarzt) mitteilen muss. Außerdem ist sichergestellt, dass nur der vom Patienten bestimmte Absender die Dokumente lesen kann.

Der Mechanismus der nicht-adressierten Kommunikation ermöglicht es außerdem, patientenbezogene Fallakten anzulegen. Hierzu können die für einen Fall relevanten Dokumente von der an der Behandlung des Patienten beteiligten Ärzten in einer temporären Akte auf dem PaDok-Server hinterlegt werden. Der Patient selbst hat auf der Grundlage des oben beschriebenen Verfahrens zu jedem Zeitpunkt seiner Behandlung die Entscheidung darüber, welcher behandelnde Arzt Dokumente seiner Fallakte einsehen kann.

## **2. Die "Elektronische Patientenakte" (EPA)**

Der Begriff "Elektronische Patientenakte" wird in unterschiedlichen Ausprägungen verwendet. Zum einen wird unter einer Elektronischen Patientenakte eine Sammlung medizinischer Informationen zu einem Patienten innerhalb einer Institution auf digitalen Datenträgern verstanden. Dies kann die Krankenakte über einen Patienten in einem Krankenhaus sein, aber auch die ärztliche Dokumentation in einer Praxis. Daneben wird der Begriff zunehmend auch werbewirksam von kommerziellen Anbietern benutzt. Sie bieten an, medizinische Daten über eine Person über das Internet zur Verarbeitung oder/und zum Abruf durch einen Arzt, Krankenhaus etc. bereitzuhalten. Im Rahmen der Diskussion der Reform im Gesundheitswesen wird allerdings der Begriff in einer anderen Bedeutung verwendet. Unter einer "elektronischen Patientenakte" ist dabei die jederzeit verfügbare, institutionsübergreifende und unter Kontrolle

des Patienten und (eines) Arztes befindliche Kopie aller relevanten Daten der Krankengeschichte zu sehen. Auf der Basis dieser Definition wurden von verschiedenen Gruppen beispielsweise "Junge Mediziner in der SPD", Konzepte entwickelt, die einerseits die Vorteile der informationstechnischen Verarbeitung medizinischer Daten nutzen und andererseits durch den Einsatz von datenschutzfreundlichen Techniken den Datenschutz und die Datensicherheit für diese Informationen sichern will.

Die Grundkonzeptionen aller EPA-Modelle geht dabei von einer Kombination einer Chipkarte mit Schlüsselfunktion und einem gesicherten Zugang zu pseudonymisierten Daten aus. In den vorgestellten Projekten sollen folgende technische Maßnahmen den Datenschutz sicherstellen:

- Nur mit einer Chipkarte und der Einwilligung des Patienten ist ein Zugang zu seiner EPA technisch überhaupt möglich.
- Die Einwilligung kann auf einzelne Ärzte oder Krankenhäuser beschränkt werden.
- Ein Widerruf ist jederzeit möglich, auch die Löschung aller Daten ist auf Wunsch des Patienten vorgesehen.

Die Modelle variieren dahingehend, dass der Ort der Speicherung der Daten, beispielsweise auf der Chipkarte des Patienten oder auf zentralen und dezentralen, regionalen Servern und der Umfang der medizinischen Daten (Arztbrief, Rezept, Röntgenaufnahmen etc.) verschieden ist.

Der Zugang zu den medizinischen Daten steht allerdings immer unter der Prämisse, dass keine Daten ohne Karte des Patienten aus dem System gelangen können und damit von Unbefugten, also auch Ärzten, gelesen werden können, d.h., der Patient kontrolliert den Zugang zu seinen Daten. Eingeschränkt wird dieser Zugang des Patienten in manchen Modellen dadurch, dass für den Zugang auch ein Arzt benötigt wird. Die Speicherung der medizinischen Daten erfolgt in der Regel in pseudonymisierter Form.

Technisch wird der Zugang zu den medizinischen Daten mit Hilfe von Verschlüsselungsverfahren sichergestellt. Ein Modell geht dabei von folgendem Verfahren aus:

Die medizinischen Daten werden auf einem regionalen Server, beispielsweise in einem Krankenhaus verschlüsselt gespeichert. Zur Pseudonymisierung der Daten erzeugt die Software auf der Chipkarte des Versicherten einen Code, der den Zugang zu Daten ermöglicht, d.h. (selbst) der Rechner des Arztes kennt nicht das Pseudonym des Patienten. Mit Hilfe des Codes, also weder mit dem Namen des Patienten, noch seinem Pseudonym, werden Daten von einem (regionalen) Server angefordert oder geschrieben. Zur Absicherung des Abrufes und/oder der Verarbeitung von Daten muss zunächst die Authentifizierung des Arztes mit Hilfe einer Health Care Professional Card erfolgen, sowohl beim (regionalen) Server wie gegenüber der Patientenchipkarte. Die Einwilligung des Patienten zu der Verarbeitung bzw. zum Abruf der Daten wird über die Vorlage bzw. Benutzung der Patientenchipkarte realisiert. Damit sichergestellt wird, dass ein Widerruf der Verarbeitung der Daten möglich ist, wird zudem auf der Karte des Patienten ein Code generiert, der den Arzt zur Datenabfrage /Datenverarbeitung berechtigt („upload code“). Mit Hilfe dieses UPLOAD-Code kann ein Arzt allerdings nur eine befristete Zeit beispielsweise 3 Monate auf die Daten des Patienten zugreifen, danach erlischt dieses Recht, der UPLOAD-Code wird ungültig. Die Übertragung der Daten zum bzw. vom Server wird zudem über Session-Keys verschlüsselt. Geht der Patient im Rahmen einer Behandlung zu einem anderen Arzt, kann dieser bei Vorlage der Patientenchipkarte und bei Freigabe der Daten durch den einstellenden Arzt befristet auf die Daten zugreifen.

Die der EPA zugrunde liegen Modelle sehen in allen Fällen einerseits die Verarbeitung von medizinischen Daten zu besseren und wirtschaftlicheren Versorgung des Patienten vor, anderseits soll durch die Pseudonymisierung der Daten anderen Bedarfsträgern (Gesundheitsministerium, Krankenkassen, Forschung und Wissenschaft) die Möglichkeit gegeben werden, statistische Auswertung auf den Daten durchführen zu können. Aus Gründen des Datenschutzes kann auch eine Pseudonymisierung der Arztdaten in diesen Datensätzen vorgesehen werden. Modellversuche mit einer (größeren) Anzahl von Patienten und Ärzten bzw. medizinischen Institutionen stehen noch aus.