

Rechtsgutachten

„Klärung haftungsrechtlicher Fragestellungen, die auf Seiten von Ärzten, Betreibern und Providern bei der Nutzung bzw. dem Betrieb einrichtungsübergreifender elektronischer Patientenakten (eEPA) entstehen.“

von Rechtsanwalt Dr. Ivo Geis

2099 Hamburg

Glockengießerwall 26

Tel. 040/30 10 41 26

E-Mail: Geis@ivo-geis.de

www.ivo-geis.de

Inhalt

Beauftragung des Gutachtens	Fehler! Textmarke nicht definiert.
Einleitung	4
1.0 Der gesetzliche Schutz von Gesundheitsdaten	5
1.1 Schutz von Patientendaten durch das Bundesdatenschutzgesetz	5
1.2 Ärztliche Schweigepflicht und Zugriffsschutz	6
1.3 Ergebnis	7
2.0 Die elektronische Kommunikation: das Haftungsrisiko auf der primären Ebene	8
2.1 Das Signaturgesetz	8
2.2 Die elektronische Signatur	9
2.3 Die fortgeschrittene elektronische Signatur	9
2.4 Die qualifizierte elektronische Signatur	10
2.4.1 Sicherheitsanforderungen an die qualifizierte elektronische Signatur	10
2.4.2 Qualifizierte Zertifizierungsdienste	11
2.4.3 Die Vergabe der qualifizierten elektronischen Signatur	11
2.4.4 Das Zertifikatverzeichnis	12
2.4.5 Zeitstempel und der Beweis des Zugangs	12
2.5 Die qualifizierte elektronische Signatur im Gesundheitswesen	12
2.5.1 Die gesetzliche Schriftform	13
2.5.2 Die elektronische Urkunde der ZPO	13
2.5.3 Elektronische Dokumentation im Sozialversicherungsrecht	14
2.5.4 Die Empfehlungen der Projekte ArchiSig, Nestor und TransiDoc	14
2.5.5 Zugriffsschutz durch Verschlüsselung	16
2.5.6 Die elektronische Gesundheitskarte und die eEPA	17
2.6 Ergebnis	17
3.0 Die elektronische Dokumentation: das Haftungsrisiko auf der sekundären Ebene	18
3.1 „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“	19
3.1.1 Ordnungsmäßige Speicherformate	19
3.1.2 Ordnungsmäßige Speichermedien	21
3.1.3 Ordnungsmäßige Wiedergabe durch Indexierung	23
3.2 „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“	24
3.2.1 Der Datenzugriff	24
3.2.2 Die maschinelle Auswertbarkeit	25
3.2.3 Die Neusignierung qualifizierter elektronischer Signaturen	25
3.3 Der Nestor-Kriterienkatalog und der Code of Practice des VOI	26
3.4 Verschlüsselung	27
3.5 Beweisrechtliche Konsequenzen für den Arzthaftungsprozess	27
3.6 Beschlagnahmeverbot	28
3.7 Haftungsrechtliche Risikominimierung der Dokumentation	29
3.8 Ergebnis	30
4.0 Der Provider als Auftragsdatenverarbeiter	31
4.1 Datenverarbeitung im Auftrag	31
4.1.1 Datenverarbeitung als Hilfsfunktion	31
4.1.2 Pflichten des Auftraggebers	31
4.1.3 Auftragserteilung	32
4.1.4 Weisungsbindung des Auftragnehmers	32
4.1.5 Konsequenzen für die primäre Ebene der behandelnden Ärzte	33
4.2 Die Konsequenzen der ärztlichen Schweigepflicht für den Provider	33
4.3 Ergebnis	34

5.0	Die Datentreuhänder-Lösung, Datenschutz und Beschlagnahmeschutz	35
5.1	Datentreuhänderschaft	35
5.2	Datenschutzrechtliche Probleme	35
5.2.1	Informationelle Gewaltenteilung	36
5.2.2	Datentreuhänderschaft und das Problem der Einwilligung	37
5.2.3	Auskunftsanspruch	38
5.3	Beschlagnahmeschutz	39
5.4	Ergebnis	40
6.0	Haftungsrisiken des einstellenden und des abrufenden Arztes	41
6.1	Einstellender Arzt	41
6.2	Abrufender Arzt	41
6.3	Ergebnis	42
7.0	Die elektronische Gesundheitskarte in der gesetzlichen Krankenversicherung	43
7.1	Angaben und Anwendungen der elektronischen Gesundheitskarte	43
7.2	Die informierte Einwilligung der Versicherten	44
7.3	Zugriff der Angehörigen eines Heilberufs	44
7.4	Rechte der Versicherten	45
7.5	Ergebnis	46
8.0	Ergebnis	48
8.1	Die zentrale Stelle und das Datenschutzrecht	48
8.2	Haftungssicherheit der elektronischen Kommunikation	48
8.3	Haftungssicherheit der elektronischen Dokumentation	48
8.4	Der Provider als Auftragsdatenverarbeiter	49
8.5	Die Datentreuhändlerlösung	49
8.6	Haftungsrisiken des einstellenden und des abrufenden Arztes	50
8.7	Die elektronische Gesundheitskarte in der gesetzlichen Krankenversicherung	50
	Abkürzungen	52
	Literatur	52

Einleitung

In Arztpraxen und Krankenhäusern, der primären Ebene der Behandlung, wird die elektronische Patientenakte (EPA) eingesetzt. Auf einer sekundären Ebene soll die einrichtungübergreifende elektronische Patientenakte (eEPA) entstehen. Die EPA in Arztpraxen und in einem Krankenhausinformationssystem (KIS) steht in engem Zusammenhang mit den konkreten Behandlungen der Patienten. Sie wird gewöhnlich durch andere medizinische Dokumente wie Arztbriefe dritter Ärzte, Laborergebnisse, Krankenhausentlassungsberichte und Reha-Abschlussberichte ergänzt. Für die EPA ist charakteristisch, dass sie nicht extern vernetzt ist und damit ein Online-Zugriff von Stellen außerhalb nicht möglich ist. Im Gegensatz hierzu ist die eEPA eine Sammelstelle von Behandlungsdokumenten, auf die dem einstellenden Arzt und anderen Ärzten ein Online-Zugriff möglich ist. Damit soll sie in zukünftigen Fällen die Behandlung verbessern und beschleunigen. Es ist vorgesehen, dass eine zentrale Stelle die Dokumente für die eEPA sammelt. Sie stellt das eEPA-System den einstellenden und abrufenden Ärzten zur Verfügung. Diese Funktion beinhaltet eine komplexe rechtliche Verantwortung. Gesundheitsdaten gelten als sensibel. Damit steht der datenschutzrechtliche Aspekt im Vordergrund (1.0). Das eEPA-System entsteht durch elektronische Kommunikation (2.0) und Dokumentation (3.0). Das Verfahren wird von der Anforderung der ärztlichen Schweigepflicht bestimmt. Wenn der Provider diese Anforderung erfüllt durch die Verwaltung verschlüsselter Daten erfüllt, dann ist eine zentrale Stelle verzichtbar (4.0). Die Alternative zur Verwaltung verschlüsselter Daten durch einen Provider ist das Konzept der Datentreuhänderschaft (5.0). Die Haftungsrisiken der einstellenden und abrufenden Ärzte werden durch eine Freizeichnungsklausel geregelt (6.0). Für den Bereich der gesetzlichen Krankenversicherung besteht eine Regelung zur elektronischen Gesundheitskarte, die auf ihre Auswirkung auf die eEPA zu untersuchen ist (7.0).

1.0 Der gesetzliche Schutz von Gesundheitsdaten

Gesundheitsdaten werden nach den Regeln des Datenschutzrechts (1.1) und der durch das Strafrecht bestimmten ärztlichen Schweigepflicht geschützt (1.2). Damit besteht im Ergebnis ein doppelter gesetzlicher Schutz für Gesundheitsdaten (1.3).

1.1 Schutz von Patientendaten durch das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) schützt personenbezogene Daten, die in oder aus Dateien verarbeitet und genutzt werden. Datenschutz bedeutet, dass das Erheben, die Speicherung und die Verarbeitung personenbezogener Daten nur unter bestimmten Bedingungen und Grenzen zulässig ist. Das BDSG hat entsprechend der Vorgabe durch die EG-Datenschutzrichtlinie gemäß § 3 Abs. 9 die Gesundheitsdaten als besondere Art personenbezogener Daten bewertet und für diese Daten einen besonderen Schutz bestimmt.¹ Diesen Schutz gewährt § 28 Abs. 7 BDSG. Hiernach ist das Erheben von Gesundheitsdaten zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. § 28 Abs. 7 BDSG bezieht präventive Untersuchungen ebenso ein wie diagnostische Maßnahmen, therapeutische Behandlungen, Nachsorgevorkehrungen und den administrativen Teil der medizinischen Versorgung. Gesundheitsdaten können deshalb sowohl für Behandlungs- als auch für Abrechnungszwecke erhoben, verarbeitet oder genutzt werden.² Der entscheidende Maßstab ist der Zweck des jeweiligen Behandlungsvertrages.³ Dieser Zweck bestimmt auch die Übermittlung der Daten zwischen den medizinischen Abteilungen einer Klinik oder zwischen Kliniken. Gesundheitsdaten müssen nach § 28 Abs. 7, Satz 2 BDSG durch Personen verarbeitet werden, die an die ärztliche oder eine entsprechende Geheimhaltungspflicht gebunden sind. Damit unterliegt auch die Verarbeitung und Nutzung der Gesundheitsdaten den Geheimhaltungspflichten des ärztlichen Personals oder sonstiger Personen, die zu einer entsprechenden Geheimhaltung verpflichtet sind. Gesundheitsdaten dürfen im Rahmen des

¹ Siehe zu den besonderen Arten personenbezogener Daten im allgemeinen *Gola/Schomerus*, BDSG, § 3 Rz. 56 und im besonderen zu den Gesundheitsdaten *Simitis*, in: *Simitis*, BDSG, § 3 Rdnr. 260

² Hierzu *Simitis*, in: *Simitis*, BDSG, § 28 Rdnr. 338-343.

³ Zum Behandlungsvertrag als Grundlage der Datenerhebung siehe *Schirmer*, in: *Rossnagel*, Handbuch Datenschutzrecht, S. 32-40.

§ 28 Abs. 7 BDSG nur im Zusammenhang mit der jeweiligen Behandlung weitergegeben werden. Das Interesse für zukünftige Behandlungen, eine breite Informationsbasis zu schaffen, berechtigt nicht zum Erheben, Verarbeiten und Nutzen von Gesundheitsdaten nach § 28 Abs. 7 BDSG. Diese Vorschrift ist nur eine begrenzt nutzbare Verwendungsgrundlage und deshalb kein Anknüpfungspunkt für einen ungehinderten Informationsaustausch mit jeder an Gesundheitsdaten interessierten Institution.⁴ Eine Datenverarbeitung über die Grenzen des Behandlungsvertrages hinaus ist nur auf Grund einer Einwilligung des Patienten zulässig. Im Ergebnis bedeutet dies für die Dokumentation von Gesundheitsdaten in Form einer eEPA, dass der Rahmen der Datenverarbeitung durch den Behandlungsvertrag bestimmt wird und wenn die Verarbeitung über diese Grenzen hinausgeht, die Einwilligungserklärung des Patienten erforderlich ist. Dieser datenschutzrechtliche Grundsatz hat eine für die Praxis wichtige Ausnahme: die ärztliche Dokumentationspflicht, zu der unter Ziffer 3.0 Stellung genommen wird. Dies bedeutet, dass das Recht zur elektronischen Dokumentation von Gesundheitsdokumenten im Rahmen der Dokumentationspflicht besteht und der Zugriff für Behandlungszwecke berechtigt ist, ohne dass hierfür die Einwilligung des Patienten vorliegen muss.

1.2 Ärztliche Schweigepflicht und Zugriffsschutz

Gemäß § 1 Abs. 3 Satz 2 BDSG bleibt die Verpflichtung zur Wahrung des ärztlichen Berufsgeheimnisses (§ 203 StGB) unberührt. Das strafrechtliche Gebot der ärztlichen Schweigepflicht gemäß § 203 StGB ist eindeutig: Das unbefugte Offenbaren eines anvertrauten fremden Geheimnisses ist strafbar. Die Übermittlung von Gesundheitsdaten ist nur zulässig, wenn sie "befugt" offenbart werden.⁵ Eine Befugnis zur Offenbarung kann auf Grund einer gesetzlichen Vorschrift oder auf Grund der Einwilligung des Patienten bestehen.⁶ Zum Offenbaren gehört nicht nur das gesprochene Wort, sondern auch schlüssiges Verhalten oder ein Unterlassen. Dann ist Offenbaren auch gegeben, wenn eine Situation geschaffen wird, in der Unberechtigte auf die Gesundheitsdaten zugreifen können. Ärztliche Schweigepflicht bedeutet damit, dass Gesundheitsdaten nur von Ärzten und deren Hilfspersonen im Zusammenhang mit dem Behandlungsvertrag verarbeitet werden können.⁷

⁴ *Simitis*, in: *Simitis*, BDSG, § 28 Rdnr. 343.

⁵ *Ulsenheimer*, in: *Laufs/Uhlenbruck*, Handbuch des Arztrechts, § 70, Rz. 1-9; siehe auch zur ärztlichen Schweigepflicht *Laufs*, *Arztrecht*, Rz. 294-320 und *Schirmer*, in: *Rossnagel*, Handbuch Datenschutzrecht, S. 32-40.

⁶ Einen Überblick über die Rechte zur Offenbarung bietet *Schlund*, in: *Laufs/Uhlenbruck*, Handbuch des Arztrechts, § 75, Rz. 1-73.

⁷ *Walz* in: *Simitis*, BDSG § 11Rdnr. 33.

Dies hat Konsequenzen für die Phase des Transports der Daten durch das Netz und die Phase der Dokumentation. In beiden Fällen müssen die Daten vor dem Zugriff nicht-ärztlichen Personals sicher sein. Eine mögliche technische Lösung ist die Verschlüsselung der Gesundheitsdaten. Zu dieser Verschlüsselungstechnik ist in Ziffer 2.6 für die Transportphase und in Ziffer 3.4 für die Dokumentationsphase Stellung genommen.

1.3 Ergebnis

Der Rahmen der Datenverarbeitung von Gesundheitsdaten wird durch den Behandlungsvertrag bestimmt. Geht die Datenverarbeitung über diesen Zweck hinaus, so ist die Einwilligung des Patienten erforderlich. Werden die Daten gespeichert, um die Dokumentationspflicht zu erfüllen, so begründet dies das Recht zur Speicherung, ohne dass die Einwilligung des Patienten hierfür erforderlich ist. Aus der ärztlichen Schweigepflicht des Strafrechts ergibt sich die Anforderung, dass die Gesundheitsdaten während des elektronischen Transports und der elektronischen Dokumentation vor dem Zugriff nicht-ärztlichen Personals sicher sein müssen. Diese Anforderung kann durch die Verschlüsselungstechnik realisiert werden.

2.0 Die elektronische Kommunikation: das Haftungsrisiko auf der primären Ebene

Die behandelnden Ärzte auf der primären Ebene haben ein Interesse an der haftungssicheren elektronischen Kommunikation mit der die Gesundheitsdaten speichernden Stelle auf der sekundären Ebene. Das Kriterium für die Haftungssicherheit der elektronischen Kommunikation mit Gesundheitsdaten sind elektronische Signaturen. Diese stehen in unterschiedlichen Qualitäten zur Verfügung, die durch das Signaturgesetz (2.1) definiert worden sind:

- die elektronische Signatur (2.2)
- die fortgeschrittene elektronische Signatur (2.3)
- die qualifizierte elektronische Signatur (2.4).

Vor dem Hintergrund gesetzlich geregelter Anwendungen soll die qualifizierte elektronische Signatur im Gesundheitswesen durch das Gesundheitskartenprojekt eingeführt werden. Die Verschlüsselung ergänzt die qualifizierte elektronische Signatur, indem sie die Nachricht vor dem Zugriff Unberechtigter schützt. Die Sicherheitstechnik der qualifizierten elektronischen Signatur und der Verschlüsselung ist in das Projekt der elektronischen Gesundheitskarte übernommen worden, um sie für den Nutzer rechtssicher und haftungssicher zu gestalten. Nach langwierigen Vorarbeiten steht die elektronische Gesundheitskarte vor dem Ausrollen. In dieses Projekt ist die eEPA als ein Datenspeicher integriert, auf den von der primären Ebene der behandelnden Ärzte aus mit der elektronischen Gesundheitskarte zugegriffen werden kann (2.5). Im Ergebnis bilden die elektronische Gesundheitskarte und die eEPA eine strategische Allianz (2.6).

2.1 Das Signaturgesetz

Das Signaturgesetz hat mehrere Entwicklungsphasen durchlaufen. Am 1. August 1997 ist das Gesetz zur digitalen Signatur in Kraft getreten, das im Rahmen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) verabschiedet worden ist.⁸ Die Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (EGSRL)⁹ stellt eine EU-einheitliche Infrastruktur für elektronische Signaturen sicher, die nach Art. 5 EGSRL der Unterschrift gleichgestellt werden. Die Anforderungen sind in das neue deutsche Signaturgesetz (SigG) integriert worden, das am 22. Mai 2001 in Kraft getreten ist¹⁰ und durch Art. 4 des Gesetzes vom 26. Februar 2007 (BGBl I S. 179) geändert worden ist. Das

⁸ Signaturgesetz – SigG, BGBl. S. 1870 ff.

⁹ Abl. EG L Nr. 13 v. 19. Januar 2000, S. 12 ff.

Signaturgesetz wird ergänzt durch die Signaturverordnung (SigV), die von der Bundesregierung am 24. Oktober 2001 beschlossen worden ist. Mit dem Signaturgesetz werden als Sicherheitstechnik für die Integrität und Authentizität elektronischer Erklärungen die drei Signaturklassen der elektronischen Signatur (1.2.1), der fortgeschrittenen elektronischen Signatur (1.2.2) und der qualifizierten elektronischen Signatur (1.2.3) definiert, deren Vergabe durch das „1. Gesetz zur Anpassung des Signaturgesetzes“ vom 12.11.2004 den Möglichkeiten der elektronischen Kommunikation angepasst worden ist.¹¹

2.2 Die elektronische Signatur

Schon das Namenskennzeichen unter einer elektronischen Nachricht ist als elektronische Signatur im Sinne von § 2 Nr. 1 SigG zu bewerten. Nach dieser Vorschrift wird nur verlangt, dass Daten anderen elektronischen Daten beigefügt sind und zur Authentifizierung dienen. Damit hat dieses Verfahren eine nur geringe Authentizitätsfunktion. Es bleibt der Zweifel, ob der Absender seinen Namen unter die elektronische Nachricht gesetzt hat oder einen anderen Namen missbraucht hat. Eine weitere Schwäche liegt in der mangelnden Integritätsfunktion: Die elektronische Signatur erfasst nicht den Text und macht damit Verfälschungen nicht erkennbar.¹²

2.3 Die fortgeschrittene elektronische Signatur

Authentizitäts- und Integritätsfunktion bietet die fortgeschrittene elektronische Signatur. Die Prüf- und Signaturschlüssel der fortgeschrittenen elektronischen Signatur müssen nach § 2 Nr. 2 SigG von Zertifizierungsdiensten als vertrauenswürdigen Dritten einer Person zugeordnet werden. Dies ist der Fall, wenn unternehmensinterne oder unternehmensexterne Zertifizierungsdienste Zertifikate an die Berechtigten vergeben, § 2 Nr. 2 a) SigG. Hierdurch muss für den Empfänger die Identifizierung des Absenders möglich sein, § 2 Nr. 2 b) SigG. Dies bedeutet Authentizität. Die fortgeschrittene elektronische Signatur muss mit Mitteln erzeugt sein, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, § 2 Nr. 2 c) SigG. Durch die Verknüpfung der fortgeschrittenen elektronischen Signatur mit den Daten der signierten Nachricht muss eine nachträgliche Veränderung erkennbar sein, § 2 Nr. 2 d) SigG. Keine erkennbare Veränderung ist damit ein Indiz für die Integrität. Anforderungen an die Sicherheit der organisatorischen Prozesse der Schlüsselverwaltung und der technischen

¹⁰ Verkündet im Bundesgesetzblatt vom 21. Mai 2001 Teil I, Nr. 22.

¹¹ BGBl I 2005, 2.

¹² Geis, in: Spindler/Schmitz/Geis TDG, Einf SigG Rz. 33.

Komponenten bestehen nicht.¹³ Die fortgeschrittene elektronische Signatur ist also offen für die technische und organisatorische Ausgestaltung.

2.4 Die qualifizierte elektronische Signatur

Die qualifizierte elektronische Signatur ist eine Steigerung der fortgeschrittenen elektronischen Signatur, indem sie durch qualifizierte Zertifizierungsdienste vergeben und verwaltet wird. Durch Sicherheitsanforderungen (2.4.1), qualifizierte Zertifizierungsdienste (2.4.2), das Vergabeverfahren (2.4.3), das Zertifikatverzeichnis (2.4.4) und den Zeitstempel (2.4.5) wird die höchste Sicherheitsstufe für die Integrität und Authentizität elektronischer Erklärungen erreicht.¹⁴ Dieser technische und organisatorische Aufwand ist auch das Handicap der qualifizierten elektronischen Signatur: Wenn sie nicht gesetzlich vorgeschrieben ist, wird sie nicht eingesetzt (2.4.6). Im Ergebnis wird die Rechtssicherheit der elektronischen Kommunikation mit Gesundheitsdaten durch die Integrität, Authentizität und den Zugriffsschutz bestimmt (2.7).

2.4.1 Sicherheitsanforderungen an die qualifizierte elektronische Signatur

Die qualifizierte elektronische Signatur muss nach § 2 Nr. 2 SigG ausschließlich dem Signaturschlüssel-Inhaber zugeordnet und mit den Daten, auf die sie sich bezieht, verknüpft sein, damit eine nachträgliche Veränderung der Daten erkannt werden kann. Sicherheit wird erreicht, indem die elektronische Signatur auf einer Chipkarte vergeben wird, die nur durch ein Passwort oder ein biometrisches Merkmal des Berechtigten aktiviert werden kann, § 17 Abs. 1 SigG, § 15 Abs. 1 SigV. Diese Identifikationsdaten dürfen nicht auslesbar oder speicherbar sein, § 17 Abs. 2 SigG, § 15 Abs. 2 SigV. Für die technischen Komponenten elektronischer Signaturen wird mit der Sicherheitsqualität EAL 4+ der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit in der Informationstechnik (Common Criteria)“ und der Sicherheitsstufe „E 3 hoch“ der „Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik“ eine hohe Sicherheitsstufe verlangt. Die Zertifikate qualifizierter elektronischer Signaturen können nach § 2 Nr. 3 SigG nur durch qualifizierte Zertifizierungsdienste vergeben werden.

¹³ *Roßnagel*, NJW 2001, 1817, 1819; *ders.*, MMR 2003, 164 ff.

¹⁴ Hierzu *Geis*, in: *Spindler/Schmitz/Geis* TDG, Rz. 12-21.

2.4.2 Qualifizierte Zertifizierungsdienste

Das System der qualifizierten Zertifizierungsdienste besteht aus freiwillig akkreditierten Zertifizierungsdiensten und angezeigten Zertifizierungsdiensten.

- Akkreditierte Zertifizierungsdienste

Auf Antrag können Zertifizierungsdienste von der Regulierungsbehörde als der zuständigen Behörde akkreditiert werden, § 15 Abs. 1, Satz 1 SigG. Die Akkreditierung ist zu erteilen, wenn Zertifizierungsdienste vor Aufnahme ihrer Tätigkeit nachweisen, dass die Vorschriften nach dem Signaturgesetz und der Signaturverordnung erfüllt sind, § 15 Abs. 1 Satz 2 SigG. Akkreditierte Zertifizierungsdienste erhalten ein Gütezeichen, § 15 Abs. 1, Satz 3 SigG. Mit diesem Gütezeichen wird nachgewiesen, dass die technische und administrative Sicherheit für die qualifizierten elektronischen Signaturen umfassend geprüft worden ist, § 15 Abs. 1 Nr. 4 SigG. Diese Zertifizierungsdienste dürfen sich als „akkreditierte Zertifizierungsdiensteanbieter“ bezeichnen und im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen, § 15 Abs. 1, Satz 5 SigG.

- Angezeigte Zertifizierungsdienste

Angezeigte Zertifizierungsdienste müssen die Aufnahme der Tätigkeit der Regulierungsbehörde als der zuständigen Behörde anzeigen, § 4 Abs. 3 Satz 1 SigG. Mit der Anzeige ist gemäß § 4 Abs. 2 SigG schriftlich darzulegen, dass die erforderliche Zuverlässigkeit und Fachkunde vorhanden ist und die übrigen Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 SigG vorliegen.¹⁵

2.4.3 Die Vergabe der qualifizierten elektronischen Signatur

Die Vergabe der qualifizierten elektronischen Signatur ist durch das „Erste Gesetz zur Änderung des Signaturgesetzes“ vom 12.11.2004, in Kraft getreten am 11.1.2005, neu geregelt worden.¹⁶ Neben der nach wie vor bestehenden persönlichen Übergabe und Bestätigung (§ 5 Abs. 1 SigG) ist die Vergabe von Signaturschlüssel und Zertifikat weitgehend durch elektronische Kommunikation möglich: der Antrag, die Bestätigung der Vergabe, die Belehrung über die Rechtsrisiken durch den Zertifizierungsdienst und eine erneute Identifizierung. Nicht elektronisch möglich ist die erstmalige Identifizierung des

¹⁵ *Roßnagel*, MMR 2002, 215, 216 f.

¹⁶ BGBl I 2005, 2; hierzu *Roßnagel*, NJW 2005, 385 ff.

Antragstellers durch Vorlage eines Personalausweises, eines Reisepasses oder gleichwertiger Dokumente.

2.4.4 Das Zertifikatverzeichnis

Der Zertifizierungsdienst hat die von ihm ausgestellten Zertifikate in ein öffentliches Zertifikatverzeichnis aufzunehmen, das online abgefragt werden kann, § 5 Abs. 1 Satz 2 SigG, § 4 SigV. Der angezeigte Zertifizierungsdienst muss die ausgestellten qualifizierten Zertifikate für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens fünf weitere Jahre ab Ende des Jahres, in dem die Gültigkeit des Zertifikates endet, in dem Zertifikatverzeichnis führen, § 4 SigV Absatz 1. Diese Nachweispflicht in dem Zertifikatverzeichnis ist für akkreditierte Zertifizierungsdienste langfristiger. Sie beträgt mindestens 30 weitere Jahre ab Ende des Jahres, in dem die Gültigkeit des Zertifikates endet, § 4 Absatz 2 SigV. Das Zertifikatverzeichnis hat damit für Empfänger einer elektronischen Nachricht mit qualifizierter elektronischer Signatur eine Sicherheitsfunktion: Sie können sich langfristig der Authentizität einer elektronischen Nachricht sicher sein.

2.4.5 Zeitstempel und der Beweis des Zugangs

Mit dem Zeitstempel als Anwendungsfall der qualifizierten elektronischen Signatur bescheinigt ein Zertifizierungsdienst, dass ihm bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben, § 9 SigG. Damit verhindern Zeitstempel ein Vor- und Rückdatieren von Daten. Sie sind erforderlich, wenn ein bestimmter Zeitpunkt im Streitfall beweisheblich sein kann. Wird vor Kommunikationsbeginn ein Zeitstempel eingeholt, so kann im Streitfall nachgewiesen werden, dass die Daten zuerst bei dem Absender vorhanden waren. Um bei einem Zertifizierungsdienst einen Zeitstempel zu Daten einzuholen, genügt es, diesem die jeweilige elektronische Signatur zu den Daten online zu übermitteln.

2.5 Die qualifizierte elektronische Signatur im Gesundheitswesen

Die qualifizierte elektronische Signatur scheint bisher nicht den Durchbruch zu einer breiten Anwendung erreicht zu haben.¹⁷ Der Einsatz beschränkt sich auf Spezialgebiete wie das Mahnverfahren, den Handel mit Emissionszertifikaten, elektronische Rechnungen und den Verkehr der Notare mit Handelsregisterstellen. Im Zuge des Gesundheitskarten-Projekts soll Heilberuflern eine qualifizierte elektronische Signatur mit dem elektronischen Heilberufsausweis zur Verfügung gestellt werden. Grundlage für die Anwendung der

¹⁷ VOI Dokumenten-Management, Ziffer 5.5.13, S. 368.

qualifizierten elektronischen Signatur im Gesundheitswesen ist deren Funktion, Integrität und Authentizität zu schaffen,¹⁸ indem sie die gesetzliche Schriftform ersetzt (2.5.1) und das elektronische Dokument der Urkunde gleichstellt (2.5.2). Deshalb ist die qualifizierte elektronische Signatur für die elektronische Dokumentation der Sozialversicherungsträger (2.5.3) angeordnet. Von den Projekten ArchiSig, Nestor und Transidoc wird die qualifizierte elektronische Signatur für die elektronische Kommunikation und zur Sicherung der elektronischen Dokumentation empfohlen (2.5.4). In Verbindung mit der Sicherheitstechnik der Verschlüsselung (2.5.5) ist die qualifizierte elektronische Signatur in die elektronische Gesundheitskarte integriert (2.5.6).

2.5.1 Die gesetzliche Schriftform

Rechtswirksames Handeln ist grundsätzlich formfrei. Eine elektronische Nachricht wie die E-Mail ist damit eine rechtswirksame Willenserklärung, mit der Rechte und Pflichten begründet werden.¹⁹ Für die formfreie Willenserklärung reicht eine Erklärung aus, nach der für den Empfänger die Identität des Erklärenden erkennbar ist. Durch das "Gesetz zur Anpassung der Formvorschriften an den modernen Rechtsgeschäftsverkehr" kann die vereinbarte und die gesetzliche Schriftform durch elektronische Signaturen ersetzt werden. Zur Wahrung der durch Rechtsgeschäft bestimmten elektronischen Form genügt eine andere Signatur als die qualifizierte elektronische Signatur nach dem Signaturgesetz, § 127 Abs. 3 BGB. Dies sind elektronische Signaturen nach § 2 Nr. 1 SigG und fortgeschrittene elektronische Signaturen nach § 2 Nr. 2 SigG. Die gesetzliche Schriftform kann durch die elektronische Form ersetzt werden, § 126 Abs. 3 BGB. Der Aussteller der elektronischen Form muss dem Text seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 SigG versehen, § 126a Abs. 1 BGB.²⁰ Die qualifizierte elektronische Signatur erfüllt auch nach § 3a VwVfG, § 36a SGB I, § 87a AO die Voraussetzungen der Schriftform. Sofern eine „dauerhaft überprüfbare qualifizierte elektronische Signatur“ nach §§ 33 Abs. 5, 37 Abs. 4 VwVfG gefordert wird, kann diese Anforderung nur mit einer akkreditierten Signatur nach § 15 SigG erfüllt werden.

2.5.2 Die elektronische Urkunde der ZPO

Das Justizkommunikationsgesetz vom 28.10.2004²¹, das am 1. April 2005 in Kraft getreten ist, honoriert qualifizierte elektronische Signaturen mit höchster Beweisqualität. Danach

¹⁸ Zur Integritäts- und Authentizitätsfunktion der Gesundheitskarte: *Schirmer*, in: *Rossnagel*, Handbuch Datenschutzrecht, S. 102-105.

¹⁹ Zur zivilrechtlichen Wirksamkeit elektronischer Erklärungen siehe die Zusammenfassung von *Mehrings*, in: *Hoeren/Sieber* (Hrsg.), Handbuch MultiMediarecht Teil 13.1 – Stand: 3. Ergänzungslieferung 2005

²⁰ *Geis*, in: *Spindler/Schmitz/Geis*, TDG, § 2 SigG Rz. 3.

gelten nach § 371a Abs. 1 ZPO für private elektronische Dokumente die Vorschriften zur Beweiskraft privater Urkunden entsprechend und ist zusätzlich der Anschein der Echtheit gegeben. Damit ist die private elektronische Urkunde der öffentlichen Urkunde mit qualifizierter elektronischer Signatur gleichgestellt, die ebenfalls die Vermutung der Echtheit begründet, § 371a Abs. 2 Satz 2 i.V.m. § 437 ZPO. Ein beweisrechtliches Defizit zwischen elektronischen Dokumenten mit qualifizierter elektronischer Signatur und unterschriebenen Papierdokumenten besteht damit nicht mehr.

2.5.3 Elektronische Dokumentation im Sozialversicherungsrecht

Durch die Ergänzung des vierten Buches Sozialgesetzbuch um § 110d werden die Voraussetzungen bestimmt, unter denen die Unterlagen auf anderen maschinell verwertbaren Datenträgern als Bildträgern aufbewahrt werden können: Die qualifizierte elektronische Signatur dessen, der die Wiedergabe auf dem Datenträger oder die ursprüngliche Aufzeichnung des Textes in gespeicherter Form hergestellt hat, muss dauerhaft überprüfbar sein. Geeignet hierfür ist die qualifizierte elektronische Signatur akkreditierter Zertifizierungsdienste. Diese Regelung entspricht der „Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung“ (SRVwV). Die nach dieser Verwaltungsvorschrift verlangte Unterschrift kann durch eine qualifizierte elektronische Signatur ersetzt werden, § 41 Abs. 1 SRVwV. Schriftliche Unterlagen dürfen vor Ablauf ihrer Aufbewahrungsfrist vernichtet werden, wenn derjenige, der die bildliche Wiedergabe erzeugt hat, durch seine qualifizierte elektronische Signatur die Übereinstimmung der bildlichen Wiedergabe mit der Unterlage bestätigt und dadurch die unbemerkte Veränderung der Unterlage ausgeschlossen ist, 36 Abs. 1 Nr. 3 SRVwV.

2.5.4 Die Empfehlungen der Projekte ArchiSig, Nestor und TransiDoc

Die Dokumentationen der Projekte ArchiSig, Nestor und TransiDoc empfehlen den Einsatz qualifizierter elektronischer Signaturen.

- **ArchiSig**

²¹ BT-Drucksache 15/4067.

Im Rahmen des Projekts ArchiSig wurden die Anforderungen und Lösungsmöglichkeiten für langfristige elektronische Archivierung signierter Dokumente untersucht und die Möglichkeit geschaffen, in IS-HMed erstellte Arztbriefe elektronisch zu signieren. Elektronisch signierte Arztbriefe werden mit zusätzlichen Verifikationsdaten, wie Zertifikat und Zeitstempel, vervollständigt. Die Zertifikate werden vom Zertifizierungsdienst der DATEV ausgestellt. Die notwendige Public Key Infrastructure wurde im Universitätsklinikum Heidelberg unter Einbeziehung der DATEV aufgebaut. Die elektronische Signatur wird mit Hilfe der Signaturschlüssel, die auf Smartcards gespeichert sind, in jedem Einzelfall immer wieder unterschiedlich erzeugt. Die klinischen Arbeitsplatzrechner sind mit Smartcard-Lesegeräten ausgestattet. Die Arztbriefe werden als Word-Dokumente angelegt und bearbeitet. Vor der Signaturerzeugung wird das Word-Dokument in ein PDF-Dokument konvertiert, das angezeigt wird. Nach der inhaltlichen Kontrolle kann der Arztbrief elektronisch signiert werden. Hierzu wird der Nutzer aufgefordert, seinen elektronischen Mitarbeiterausweis in das Lesegerät zu stecken und sein Kennwort einzugeben. Zusätzlich zum PDF-Dokument werden alle vorhandenen elektronischen Signaturen mit dem Signaturdatum und dem Signaturstatus angezeigt. Ist der Arztbrief erstellt, kann er durch Ändern des Dokumentenstatus archiviert werden. Die Archivierungsfunktion sammelt alle Zertifikate, die zur Verifikation der Signaturen gebraucht werden, verifiziert diese und fügt sie dem zu archivierenden Dokument bei. Dann wird ein erweiterter Zeitstempel eingeholt und dem Dokument hinzugefügt. Die Neusignierung wird vor Ablauf der Sicherheitseignung eines verwendeten Algorithmus, die von der Bundesnetzagentur im Bundesanzeiger veröffentlicht wird, durch ein automatisches Verfahren angestoßen. Es gehört zur Sorgfaltspflicht eines Archivsystembetreibers, dass regelmäßig geprüft wird, ob eine Neusignierung durchzuführen ist. Der ArchiSig-Prototyp wird seit August 2003 in der Universität Heidelberg in den Stationen und Ambulanzen der Abteilung Innere Medizin II für das elektronische Signieren von Arztbriefen in der klinischen Routine eingesetzt.²²

- **Der Nestor-Kriterienkatalog**

Nach dem „Nestor Kriterienkatalog vertrauenswürdige digitale Langzeitarchive“ kann nach Ziffer 7.1 in bestimmten Kontexten durch die Verwendung digitaler Signaturen die Authentizität der Übergabeobjekte sichergestellt werden. Nach Ziffer 7.3 registriert sich das digitale Langzeitarchiv bei einer autorisierten Stelle, z.B. bei der Bundesnetzagentur und erhält dort ein digitales Signaturschlüssel-Zertifikat, um es zum Erzeugen digitaler Signaturen

²² *Roßnagel/Schmücker*, Beweiskräftige elektronische Archivierung, Ziffer 14.3, S. 165-175.

zu benutzen. Nestor empfiehlt den Einsatz qualifizierter elektronischer Signaturen für die Archivierung von Patentanmeldungen.²³

- **Die TransiDoc-Grundsätze**

Nach Ziffer 3 der TransiDoc-Grundsätze sind, um die Urheberschaft zu sichern, bei der Transformation elektronisch signierter Dokumente die Signaturen des Ausgangsdokuments zu verifizieren und ist das Ergebnis dieser Prüfung festzuhalten. Alle benötigten Verifikationsdaten wie Zertifikate, Sperrlisten, Zertifikatsstatusabfragen, Zeitstempel sind zu beschaffen. Nach Ziffer 5 muss die Transformation dem ausführenden Bearbeiter zugerechnet werden können. Die Zurechenbarkeit wird durch eine elektronische Signatur mit ausreichend hohem Sicherheitsniveau erreicht. Qualifizierte elektronische Signaturen mit Anbieterakkreditierung nach dem Signaturgesetz sollten eingesetzt werden, falls ein hoher Beweiswert langfristig erforderlich ist.

2.5.5 Zugriffsschutz durch Verschlüsselung

Zur Rechtssicherheit der elektronischen Kommunikation mit Gesundheitsdaten gehört nicht nur die Integrität und Authentizität des Dokuments, sondern auch wie in Ziffer 1.0 ausgeführt wegen der Anforderungen des Datenschutzrechts und der ärztlichen Schweigepflicht der Schutz vor dem Zugriff Unberechtigter. Die qualifizierte elektronische Signatur sichert die Integrität der Daten und die Authentizität des Dokuments, nicht aber den Schutz vor dem Zugriff Unberechtigter während des Transports und der Archivierung. Die technische Lösung für den Zugriffsschutz ist die asymmetrische Verschlüsselung (Public-Key-Verfahren) der Gesundheitsdaten.²⁴ Bei einer asymmetrischen Datenverschlüsselung werden verschiedene Schlüssel zum Verschlüsseln und Entschlüsseln verwendet. Zum Verschlüsseln dient der öffentliche Schlüssel (public key), der von einem potenziellen Empfänger bekannt gegeben wird. Zum Entschlüsseln dient der private Schlüssel (private key), der von seinem Besitzer verwahrt wird und auf den kein anderer Zugriff haben darf. Aus dem öffentlichen Schlüssel lässt sich der private Schlüssel nicht ableiten und allein aus dem öffentlichen Schlüssel lässt sich die verschlüsselte Nachricht nicht dechiffrieren.²⁵ Damit sind die Gesundheitsdaten wie in einem virtuellen Container dem Zugriff Unberechtigter entzogen. Eine Pflicht zur

²³ Nestor-Kriterienkatalog, Ziffer 13.2, S. 29.

²⁴ Hierzu *Schirmer*, in *Rossnagel*, Handbuch Datenschutzrecht, S. 81 und 99.

²⁵ Zur Technik des Public-Key-Verfahrens: Brockhaus Fachlexikon Computer, Stichwort Datenverschlüsselung.

Anwendung dieser Technik besteht nicht. So können Daten in einer Standleitung ausgetauscht werden, die sie vor dem Zugriff Unberechtigter schützt.

2.5.6 Die elektronische Gesundheitskarte und die eEPA

Das langwierige Projekt der elektronischen Gesundheitskarte scheint zu einem Abschluss zu kommen. Nach aktuellen Presseberichten sollen im Sommer dieses Jahres zunächst in Nordrhein-Westfalen die Kassenärzte mit den Lesegeräten für die Gesundheitskarte ausgestattet werden.²⁶ Das Projekt soll von diesem Bundesland aus bis zum Jahre 2010 bundesweit ausgerollt sein. Die sicherheitstechnischen Bestandteile der Karte sind qualifizierte elektronische Signatur und Verschlüsselung. Unter dem Schutz dieser Sicherheitstechnik können Ärzte und Apotheker auf Gesundheitsdaten zugreifen, die sich auf der Karte und auf anderen Datenspeichern befinden, die wie die eEPA den gesundheitlichen Lebenslauf eines Patienten dokumentieren.²⁷ In diesem Zusammenspiel mit der elektronischen Gesundheitskarte hat die eEPA ihre Position in der medizinischen Telematik eingenommen.

2.6 Ergebnis

Rechtssicherheit und damit Haftungssicherheit für die Kommunikation mit Gesundheitsdaten entsteht durch Integrität des Dokuments und durch Authentizität des Absenders. Diese Funktionen sichern qualifizierte elektronische Signaturen auf hohem Niveau. Durch Verschlüsselungen wird die ärztliche Schweigepflicht gewahrt und der Datenschutz für Gesundheitsdaten erfüllt, da der Inhalt des elektronischen Dokuments vor dem Zugriff Unberechtigter gesichert ist. Diese Anforderungen werden durch die elektronische Gesundheitskarte erfüllt, die aktuell realisiert werden soll. Die elektronische Gesundheitskarte erlaubt den Zugriff auf Gesundheitsdaten, die auf der Karte und auf anderen Datenspeichern, wie der eEPA, dokumentiert sind. Hierdurch ist eine strategische Allianz zwischen der elektronischen Gesundheitskarte und der eEPA begründet.

²⁶ Auf dieses Projekt weisen hin *Semler/Ripkens-Reinhard*, *Telemedizinführer Deutschland*, 2006, 353, 354; ausführlich zur elektronischen Gesundheitskarte *Hornung*, *Die digitale Identität*, vor allem S. 362-374 und *Schirmer*, in: *Rossnagel*, *Handbuch Datenschutzrecht*, S. 112-119.

²⁷ FAZ vom 26. März 2008, S 12, „Durchbruch für die Gesundheitskarte“.

3.0 Die elektronische Dokumentation: das Haftungsrisiko auf der sekundären Ebene

Die Folge der elektronischen Kommunikation mit Dokumenten ist deren Dokumentation auf der sekundären Ebene durch einen Provider. Für die behandelnden Ärzte auf der primären Ebene bleibt das Haftungsrisiko im Rahmen der ärztlichen Dokumentationspflicht bestehen. Im Gesundheitswesen wird die ärztliche Dokumentationspflicht als Nebenpflicht aus dem Behandlungsvertrag abgeleitet und mit dem Persönlichkeitsrecht des Patienten begründet.²⁸ Diese Dokumentationspflicht besteht auch nach der berufsständisch internen Regelung des § 10 Abs. 1 und Abs. 3 Musterberufsordnung für Ärzte (MBO).²⁹ Anforderungen an die ordnungsmäßige Dokumentation sind nicht gesetzlich oder durch Verordnungen geregelt.³⁰ Diese rechtliche Lücke kann allgemein aus den Vorschriften über die Revisionsicherheit im Handelsrecht und im Steuerrecht und speziell aus Regeln des Gesundheitswesens abgeleitet werden. Rechtliche Grundlagen für die ordnungsmäßige und damit revisions sichere Archivierung sind die Aufbewahrungsvorschriften des HGB, der AO und deren Interpretation durch das Bundesfinanzministerium. Für andere Rechtsgebiete wie das Medizinrecht bestehen keine vergleichbaren Vorschriften. Deshalb haben die handelsrechtlichen und steuerrechtlichen Anforderungen eine Vorbild- und Beispielfunktion, denn die durch die ordnungsmäßige Archivierung bezweckte Integrität und Wiedergabe der Dokumentation gilt auch für das Medizinrecht. Hierdurch werden die in der medizinischen Dokumentation bestimmenden Anforderungen der Gedächtnisstütze, der Kommunikationshilfe, der Beweisführung, der Kontrollmöglichkeiten und der Rechenschaftsablegung ermöglicht. Die Anforderungen an die ordnungsmäßige Archivierung nach Handelsrecht und Steuerrecht sind vom Bundesfinanzministerium durch die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) (3.1) und die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) (3.2) interpretiert worden.³¹ Ergänzend sind Anforderungen an die Archivierung von dem Code of Practice des VOI und spezifische Anforderungen für die Archivierung von Gesundheitsdaten von dem Projekt ArchiSig und dem Nestor-Kriterienkatalog definiert worden (3.3). Wie für die elektronische Kommunikation, so ist auch für die elektronische Dokumentation die Verschlüsselung der entscheidende Sicherheitsfaktor (3.4). Dieser Sicherheitsfaktor hat direkte Konsequenzen für die beweisrechtliche Qualität der Dokumente im Arzthaftungsprozess (3.5). Die archivierten

²⁸ *Roßnagel/Schmücker*, Beweiskräftige elektronische Archivierung, Ziffer 3.4.5.2, S. 27.

²⁹ *Uhlenbruck/Schlund*, in: *Laufs* (Hrsg.) Handbuch des Arztrechts, § 59 Rz. 1-4 und § 60 Rz. 17; *Laufs*, Arztrecht, Rz. 321-322.

³⁰ Zur Dokumentation nach den Grundsätzen der Ordnungsmäßigkeit *Uhlenbruck/Schlund*, in: *Laufs* (Hrsg.) Handbuch des Arztrechts, § 59, Rz. 11

Dokumente müssen vor Beschlagnahme geschützt sein (3.6) und dürfen nicht ein haftungsrechtliches Risiko bilden (3.7). Als entscheidendes Ergebnis dieses technischen und organisatorischen Aufwandes kann auf die zentrale Stelle verzichtet werden (3.8).

3.1 „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“

Im Focus der GoBS steht das gescannte Dokument. Nach den GoBS³² kommt es für die ordnungsmäßige Archivierung auf den Einsatz ordnungsmäßiger Speicherformate (3.1.1) und Speichermedien (3.1.2) und die ordnungsmäßige Wiedergabe der Dokumente (3.1.3) an.

3.1.1 Ordnungsmäßige Speicherformate

Die Aufbewahrung von Unterlagen ist ordnungsmäßig, wenn die Integrität der Dokumente gewährleistet ist und für die Dauer der Aufbewahrung die Informationen auf dem Speichermedium jederzeit abrufbar erhalten bleiben. Die Ordnungsmäßigkeit ist nicht von bestimmten Speicherformaten abhängig, denn die GoBS sind wie die Aufbewahrungsvorschriften des HGB und der AO technikneutral.³³ Für die Gesundheitsdokumente bedeutet dies, dass unproblematisch die Standardformate DICOM und HL7, die Bilddateien und in PDF konvertierte Worddokumente ordnungsmäßig sind.

- DICOM

Digital Imaging and Communication in Medicine ist ein Datenformat, das sich international als Standard für die Übermittlung von medizinischem Bildmaterial etabliert hat. In Europa ist DICOM durch das Comité Européen de Normalisation (CEN) unter ENV 12052 veröffentlicht. Transparenz und Standardisierung sind damit hoch ausgeprägt. Die Stabilität ist gering, da DICOM fortwährend erweitert und angepasst wird. Der DICOM-Standard ist von nahezu allen Anbietern von Picture Archive and Communication Systems (PACS) übernommen worden. Präsentationswerkzeuge verschiedener Hersteller stehen zur Verfügung. Das Bildformat enthält Zusatzinformationen zu aufnahmespezifischen Eigenschaften der Bilddaten, so dass die Darstellung gesichert ist. Die Datensicherheit wird durch drei Sicherheitserweiterungen gewährleistet: durch die Absicherung der Netzwerkkommunikation mit einem TLS-Protokoll, durch die Verschlüsselung einzelner

³¹ Eine Hilfe für die Interpretation der elektronischen Archivierung bietet *Roßnagel/Fischer-Dieskau/Jandt*, Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente.

³² BStBl. I 1995, S. 738.

³³ GoBS, VIII b) 1. Absatz Satz 1 und 2, in: BStBl. I 1995, S. 738, 739.

Datenfelder, um die Vertraulichkeit von Patientenidentifikationsdaten zu sichern, und durch ein proprietäres Signaturdatenformat.³⁴

- **HL7**

HL7 ist ein internationaler Kommunikationsstandard für das Gesundheitswesen. In Deutschland ist die HL7 Version 2.4 unter der DIN Norm 58965 publiziert. Version 3.0 befindet sich im Standardisierungsprozess unter ISO /HL7 DIS 21731. In HL7 wird nur die Authentizität der Nachrichten berücksichtigt. Es werden keine kryptographischen Verfahren verwendet. Die Sicherheit von HL7-Nachrichten wird durch zwei Methoden ermöglicht: Das Prinzip der Secure Messages arbeitet mit Nachrichten, die z.B. mit S/MIME gesichert sind und über unsichere Netze übertragen werden. Das Prinzip des Secure Channel überträgt ungeschützte Informationen über einen sicheren Kanal, z.B. über SSL.³⁵

- **Bildformate GIF, PNG, JPEG**

GIF, das Graphics Interchange Format, ist die Standardversion für die Speicherung von Rastergraphiken. Durch die Nutzung im Internet ist das Format weit verbreitet und wird von allen Bildverarbeitungsprogrammen unterstützt. Es existieren keine Sicherheitsmechanismen, welche die Integrität, Authentizität und Vertraulichkeit einer GIF-Graphik gewährleisten. Als Alternative zum GIF-Format wurde für Anwendungen im Internet das PNG (Portable Network Graphics) Format entwickelt. Das Programm enthält keine Mechanismen zur Sicherung von Integrität, Authentizität und Vertraulichkeit. Im Format JPEG, dem Graphikformat der Joint Photographic Experts Group, sind keine Sicherheitsmaßnahmen zur Gewährleistung von Integrität, Authentizität und Vertraulichkeit vorgesehen. Diese sollen mit dem in Entwicklung befindlichen JPEG2000-Standard JPSEC möglich gemacht werden.³⁶

- **Microsoft Word und die Konvertierung in das Format PDF**

Microsoft Word speichert die Daten in einem Format, für das Microsoft die Dokumentation eingestellt hat. Deshalb gelten Word-Dokumente als nicht geeignet, um langfristig in Archiven gespeichert zu werden. Nach den Auflagen der EU-Kommission vom März 2004 und den bestätigenden Entscheidungen des Europäischen Gerichtshofs garantiert Microsoft

³⁴ Zum DICOM-Standard: *Roßnagel/Schmücker*, Beweiskräftige elektronische Archivierung, Ziffer 7.3.4, S. 72 und Gutachten „Konventionelle Formate“, S. 39-42.

³⁵ *Roßnagel/Schmücker*, Beweiskräftige elektronische Archivierung, Ziffer 7.3.4, S. 72.

³⁶ Siehe zu dem Format JPEG: *Roßnagel/Schmücker*, Beweiskräftige elektronische Archivierung, Ziffer 7.3.2, S. 70 f.; VOI Dokumenten-Management, Ziffer 5.1.6, S. 230-237.

seinen Wettbewerbern in Zukunft die Schnittstelleninformationen zugänglich und nutzbar zu machen, die für die Entwicklung von Windows-basierter Software nötig sind. Durch diese Transparenz könnte Microsoft Word mit Blick auf die langfristige Aufbewahrung in positivem Sinne neu bewertet werden.³⁷ Deshalb wird es als notwendig angesehen, das Format für die Langzeitarchivierung zu konvertieren. So verlangen die „Grundsätze des Projektes TransiDoc“, dass das Ausgangsdokument in ein langfristig eindeutig interpretierbares, stabiles und standardisiertes Format transformiert wird. Um das Zieldokument unabhängig vom Ausgangsdokument verwenden zu können, müssen neben den transformierten Daten auch die im Transformationsprozess anfallenden Daten wie Ablaufprotokolle und Prüfergebnisse aufbereitet werden können.³⁸ Entsprechend empfiehlt der „Kriterienkatalog vertrauenswürdige digitale Langzeitarchive“ der Nestor-Arbeitsgruppe „Vertrauenswürdige Archive-Zertifizierung“ unter Ziffer 10.1 für formatierte Texte das Format PDF. Portable Document Format ist ein Datenformat, das sich zu einem De-facto-Standard für den Austausch von Textdokumenten im World Wide Web entwickelt hat, da PDF ein effektiv komprimierendes Format ist und daher schnell übertragen und angezeigt werden kann und es den seitenweisen Aufbau von größeren Downloads erlaubt.³⁹ PDF unterstützt verschiedene Sicherheitsmechanismen. Soll das Dokument vertraulich sein und nur bestimmten Nutzern zur Verfügung gestellt werden, so kann der Ersteller das Dokument über kryptographische Verfahren verschlüsseln. PDF unterstützt auch die elektronische Signatur.⁴⁰

3.1.2 Ordnungsmäßige Speichermedien

Nach den GoBS ist die Aufbewahrung von Unterlagen ordnungsmäßig, wenn die gesicherte Aufbewahrung gewährleistet ist und für die Dauer der Aufbewahrung die Informationen auf dem Speichermedium jederzeit abrufbar erhalten bleiben. Die Ordnungsmäßigkeit ist nicht von einem bestimmten Speichermedium abhängig. Zulässig und damit ordnungsmäßig im Sinne der handelsrechtlichen und steuerrechtlichen Aufbewahrungsvorschriften sind alle Speichermedien: die CD-Rom, die nicht wiederbeschreibbare Platte, die wiederbeschreibbare Platte und das Speicherband. Entscheidend für die Ordnungsmäßigkeit sind die hardwaremäßigen, softwaremäßigen und organisatorischen Sicherheitsfunktionen, die für das

³⁷ Siehe zu dem Verfahren gegen Microsoft: FAZ vom 23.10.07, S. 15 „Microsoft beugt sich der EU-Kommission“.

³⁸ Ziffer 8 der „Grundsätze des Projekts TransiDoc für die Transformation signierter Dokumente“ unter www.transidoc.de (Stand 17. September 2007).

³⁹ Brockhaus Fachlexikon Computer, Stichwort „PDF“.

⁴⁰ Zum PDF-Format siehe: *Roßnagel/Schmücker*, Beweiskräftige elektronische Archivierung, Ziffer 7.3.1, S. 67-69 ; VOI Dokumenten-Management, Ziffer 5.1.7, S. 238-242.

jeweilige Speichermedium gesondert ausgeprägt sein können.⁴¹ Nach dem Nestor „Kriterienkatalog vertrauenswürdige digitale Langzeitarchive“ legt das Archivmanagement die erforderliche Qualität der Speichermedien fest.⁴² Als Sicherung wird die persistente Speicherung auf geeigneten Medien empfohlen.⁴³ Im Ergebnis überlassen die GoBS und der Nestor-Kriterienkatalog dem Anwender die Entscheidung. Aus rechtlichen Überlegungen sollte die Entscheidung von dem Effekt für die Integrität, die Verkehrsfähigkeit und Vollständigkeit der Dokumentation bestimmt sein. Für die folgenden Speichermedien ist die Integrität, die Verkehrsfähigkeit und die Vollständigkeit der Dokumente ausgeprägt: WORM-Systeme, da die Daten nicht überschrieben werden können, Wiederbeschreibbare optische Platten, die die Sicherheit vor Manipulationen der WORM-Systeme mit kürzeren Zugriffszeiten verbinden, CD-R-Systeme, die die Sicherheit des WORM-Systems mit einem niedrigeren Preis verbinden, die DVD-R als DV-Variante des WORM-Systems.

- **WORM-Systeme**

Das Write Once Read Many System ist eine Platte, bei der die Sektoren einmal beschrieben und danach beliebig oft gelesen werden können. Das System bietet den Vorteil großer Datensicherheit, da die Daten nicht überschrieben werden können. Die Speichermethode ist damit gegen Manipulationen geschützt. Für die Speicherung von aufbewahrungspflichtigen Dokumenten sind WORM-Systeme deshalb am besten geeignet. Der Nachteil dieser Methode ist die längere Zugriffszeit.⁴⁴

- **Wiederbeschreibbare optische Platte**

Die wiederbeschreibbare optische Platte verbindet die Vorteile der WORM-Systeme mit denen der Magnetplatte. Gegenüber der Magnetplatte bietet sie eine höhere und längere Datensicherheit und ist widerstandsfähiger gegenüber Magnetfeldern, Temperaturextremen und Stoß. Gegenüber dem WORM-System bietet sie kürzere Zugriffszeiten.⁴⁵

- **CD-Systeme**

Die Compact Disk hat sich als Standard etabliert. Die Daten-CD wird für die Distribution von Software, Handbüchern, Ersatzteilkatalogen, Lexika, rechnergestützten Informations- und Unterhaltungssystemen eingesetzt. Die 12-cm CD fasst bis zu 800 MB. Es wird nicht

⁴¹ GoBS VIII.b), in: BStBl. I 1995, S. 738, 739 und F.4.16 Ziffer 1.1.2.

⁴² Nestor-Kriterienkatalog, Ziffer 6.2, S. 16.

⁴³ Nestor-Kriterienkatalog, Ziffer 10.3, S. 21.

⁴⁴ VOI Dokumenten-Management, Ziffer 5.2.8, S. 274 und Ziffer 5.2.13, S. 295.

⁴⁵ VOI Dokumenten-Management, Ziffer 5.2.8, S. 275 f.

empfohlen, diese „überlangen Medien“ für die Langzeitarchivierung zu verwenden. Ein Nachteil der CD sind die langen Zugriffszeiten. Die Sicherheit der WORM wird mit der CD-R oder auch CD-WORM genannt erreicht. Mit CD-Writeern werden CD-Datenträger beschrieben. Der Vorteil ist der niedrige Preis des Datenträgers und der CD-Jukebox, die durch einen Robotermechanismus Platten aus dem Ablagefach entnimmt und zur Bearbeitung des Inhalts in das Laufwerk einsetzt.⁴⁶ Wegen der hohen Zuverlässigkeit wird sie seit mehreren Jahren vom Europäischen Patentamt für die Speicherung und Distribution von Patentdaten verwendet. Die wiederbeschreibbare CD-RW gestattet bis zu einigen Tausend Schreibzyklen. Als Dateisystem der CD-RW hat sich UDF etabliert. Dieses Format wird wegen seiner internen Struktur als ineffizient und langsam bewertet. Die meisten UDF-Implementierungen weisen eine mangelhafte Stabilität bei Mehrfachänderungen und parallelen Schreibzugriffen auf. Deshalb wird die CD-RW als Archivmedium nicht empfohlen.⁴⁷

- **DVD-Systeme**

Weiterentwicklungen der CD-Technik sind unter der Bezeichnung CD-DVD auf dem Markt. Die DVD-R ist die WORM-Variante. Die Variante DVD-R for General Use bietet die höchste Sicherheit und ist damit das bevorzugte Archivmedium. Die Kapazität beträgt 4,7 GB pro Seite. Die nächste Generation der CD-/DVD-Technik sind Systeme mit einer Kapazität von 30 bis 40 GB, die Laser mit kurzen Wellenlängen (Blue Ray) verwenden. Bisher sind UDO (Ultra Density Optical)-Systeme von Plasmon und PDD (Professional Data Disk) von Sony auf dem Markt. Die Systeme sind nicht kompatibel. Damit sind Formatauseinandersetzungen programmiert. Klare Standards sind bisher nicht zu erwarten.⁴⁸

3.1.3 Ordnungsmäßige Wiedergabe durch Indexierung

Die Wiedergabe von aufbewahrungspflichtigen Informationen ist gemäß § 257 Abs. 3 HGB ordnungsmäßig, wenn der Zugriff innerhalb einer angemessenen Frist möglich ist und nach § 147 Abs. 2 AO, wenn der Zugriff „unverzüglich“ möglich ist. In der zivilrechtlichen Definition heißt „unverzüglich“ ohne schuldhaftes Zögern. Diese Frist für das Lesbarmachen ist analog zu § 238 Abs.1 Satz 2 HGB nach den Verhältnissen des Einzelfalles zu bestimmen.⁴⁹ Hierzu muss das Dokument mit einem Index versehen sein, unter dem es

⁴⁶ VOI Dokumenten-Management, Ziffer 5.2.9, S. 283 f.

⁴⁷ VOI Dokumenten-Management, Ziffer 5.2.8, S. 277-280.

⁴⁸ VOI Dokumenten-Management, Ziffer 5.2.8, S. 280-282.

⁴⁹ Wiedemann, in: Ebenroth/Boujong/Joost, § 257 Rdnr. 25.

aufgefunden werden kann.⁵⁰ Problematisch ist die Langfristarchivierung: Dokumente, deren Inhalt der vertraglichen oder deliktsrechtlichen Verjährung unterliegen, müssen über einen Zeitraum von mindestens 30 Jahren archiviert werden. Während dieses Zeitraums muss der Zugriff auf das Dokument möglich sein. Eine Lösung für dieses Problem muss in einem Migrationskonzept gefunden werden, durch das die Dokumente in der jeweils aktuellen Archivierungstechnologie während des Archivierungszeitraums verfügbar sind. Der von der Nestor-Arbeitsgruppe erarbeitete Kriterienkatalog für die Langfristarchivierung sieht die Verfügbarkeit der Metadaten als wesentliche Funktion für die ordnungsmäßige Wiedergabe an. Das Datenmanagement muss dazu geeignet sein, die notwendigen Funktionalitäten des digitalen Langzeitarchivs zu gewährleisten. Hierzu muss das digitale Langzeitarchiv

- zur formalen und inhaltlichen Beschreibung und Identifizierung der digitalen Objekte,
- zur strukturellen und technischen Beschreibung der digitalen Objekte,
- zur Beschreibung von Nutzungsrechten und -bedingungen

in ausreichendem Maße Metadaten erheben.⁵¹

3.2 „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“

Im Focus der „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“

(GDPdU) steht das originäre elektronische Dokument. Nach den GDPdU muss das originäre elektronische Dokument für den Datenzugriff (3.2.1) maschinell auswertbar (3.2.2) archiviert werden.⁵² Werden Dokumente mit qualifizierter elektronischer Signatur archiviert, so erfordert dies die Neusignierung, wenn die Signaturen abgelaufen sind (3.2.3).

3.2.1 Der Datenzugriff

Das Bundesfinanzministerium hat mit den GDPdU das Recht zum Zugriff auf originär digitale Unterlagen im Rahmen der Außenprüfung in Form des unmittelbaren Datenzugriffs, des mittelbaren Datenzugriffs und der Datenträgerüberlassung konkretisiert. Für den unmittelbaren Datenzugriff der Finanzbehörde muss der Steuerpflichtige nach Abschnitt I.2.a) GDPdU dem Prüfer die erforderlichen Hilfsmittel zur Verfügung stellen, damit er selbständig auf die Daten zugreifen kann. Für den mittelbaren Datenzugriff hat der Steuerpflichtige entsprechend den Angaben des Prüfers den Zugriff auf die Daten zu

⁵⁰ GoBS VIII b) 1. und VIII, 3., in: BStBl. I 1995, S. 738, 740.

⁵¹ Nestor-Kriterienkatalog, Ziffer 12, S. 22-28; siehe speziell zu den Problemen langfristiger Archivierung: *Roßnagel/Fischer-Dieskau/Jandt/Knopp*, Langfristige Aufbewahrung elektronischer Dokumente – Anforderungen und Trends, Baden-Baden 2007.

⁵² GDPdU III. 1. Satz 1, in: BStBl I 2001, S. 415.

organisieren, Abschnitt I.2.b) GDPdU. Statt des unmittelbaren und mittelbaren Datenzugriffs kann die Finanzbehörde einen Datenträger verlangen, auf dessen Daten sie zugreifen kann.

3.2.2 Die maschinelle Auswertbarkeit

Um den Datenzugriff zu ermöglichen, muss nach § 147 Abs. 2 Nr. 2 AO sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können. Damit sind originär digitale Unterlagen auf maschinell verwertbaren Datenträgern während der gesamten Aufbewahrungsfrist zu archivieren. Nach Abschnitt III.1 Satz 2 GDPdU sind originär digitale Unterlagen die in das Datenverarbeitungssystem in elektronischer Form eingehenden Daten und die im Datenverarbeitungssystem erzeugten Daten; maschinell verwertbare Datenträger sind maschinell lesbare und auswertbare Datenträger. Wenn originär digitale Unterlagen auf maschinell verwertbaren Datenträgern zu archivieren sind, dann dürfen sie nicht, so die Schlußfolgerung des Bundesfinanzministeriums, ausschließlich in ausgedruckter Form oder auf Mikrofilm aufbewahrt werden.⁵³ Die Anweisungen der GDPdU haben einen allgemeingültigen Charakter: Um Datenverlust durch Medienbruch zu vermeiden, sind originär elektronische Dokumente elektronisch zu archivieren.

3.2.3 Die Neusignierung qualifizierter elektronischer Signaturen

Nach Abschnitt „II. Prüfbarkeit digitaler Unterlagen“ müssen die qualifizierte elektronische Signatur und die Verschlüsselung überprüfbar sein. Dies erfordert, dass vor einer weiteren Verarbeitung des Dokuments die qualifizierte elektronische Signatur im Hinblick auf die Integrität der Daten und die Signaturberechtigung geprüft und das Ergebnis dokumentiert wird und die Speicherung des elektronischen Dokuments auf einem Datenträger erfolgt, der Änderungen nicht mehr zulässt. Elektronisch signierte Dokumente sind unter dem Aspekt der langfristigen Aufbewahrung ein Problemfall. Auch nach langer Zeit muss das signierte Dokument lesbar sein und es muss die Integrität und Authentizität nachgewiesen werden können. Die Hash- und Signaturverfahren verlieren im Laufe der Zeit durch Entwicklungen der Rechnerschnelligkeit und Kryptoanalyse ihre Sicherheitseignung und gefährden damit die Integrität des Dokuments. Die Neusignierung ist bei großen Archiven problematisch, da sie in einem automatisierten Prozess erfolgen muss. Die Urheberschaft einer Signatur lässt sich langfristig nur durch Verifikationsdaten in Form von Zertifikaten und deren Bestätigung

⁵³ GDPdU III. 1., in: BStBl. I 2001, S. 415.

durch Zertifizierungsdienste nachweisen. Dieses Risiko kann durch Signaturen akkreditierter Zertifizierungsdienste minimiert werden, da diese Zertifikate mindestens 30 Jahre nach Ablauf des Gültigkeitsjahres nachprüfbar aufzubewahren sind. Die langfristige Lesbarkeit wird in der Praxis sichergestellt, indem alte Hard- und Software mit neuen Systemen emuliert wird oder die Dokumente auf neue Systeme konvertiert werden. Damit geht die ursprüngliche Signatur verloren. Durch eine vertrauenswürdige Stelle muss bestätigt werden, dass das Zieldokument dem Ausgangsdokument entspricht. Dies ist für den Verwaltungsbereich nach § 33 Abs. 4, 5 VwVG durch eine elektronische Beglaubigung geregelt worden.⁵⁴

3.3 Der Nestor-Kriterienkatalog und der Code of Practice des VOI

Der Nestor –Kriterienkatalog und der Code of Practice des VOI haben Sicherheitsanforderungen formuliert, die als Anregung verstanden werden können, den unbestimmten Rechtsbegriff der ordnungsmäßigen Archivierung zu interpretieren.

- Der Nestor-Kriterienkatalog

Bei der elektronischen Archivierung sind die Sicherheitsanforderungen des Objektmanagements zu berücksichtigen: die Sicherung der Integrität der Objekte, d.h. Schutz vor Modifikationen durch beabsichtigte und unbeabsichtigte menschliche Aktionen sowie technische Unvollkommenheit, die Sicherung der Authentizität der Objekte, die Sicherung der Vertraulichkeit der Objekte, d.h. Ausschluss unerlaubter Informationsbeschaffung, die Sicherung der Verfügbarkeit der Objekte durch die Verfügbarkeit der Funktionalitäten des Objektmanagements (z.B. Schutz vor Sabotage, Ausfällen des Systems).⁵⁵

- Der Code of Practice des VOI

Unter Sicherheit werden folgende Funktionen verstanden: Vertraulichkeit der Daten, Authentizität und Integrität der Daten, Schutz der Daten gegen Veränderungen, Schutz der Daten gegen Verlust, Verfügbarkeit der Systeme und Daten, Katastrophenfall-Planung. Vertraulichkeit der Daten wird durch die Vergabe von Zugriffsrechten erreicht und auf einer höheren Ebene durch Verschlüsselung. Die Wahl bestimmter Speichermedien wie WORM, CD-R oder DVD-R unterstützt den Schutz der Daten vor Veränderung. Prüfsummen, Signaturen und Zeitstempel sind eine sinnvolle Ergänzung. Für den Schutz der Daten gegen Verlust ist eine adäquate Sicherung und Lagerung der Daten erforderlich. Verfügbarkeit der

⁵⁴ *Roßnagel/Schmücker*, Beweiskräftige elektronische Archivierung, Ziffer 3.5, S. 28-35.

⁵⁵ Nestor-Kriterienkatalog, Ziffer 13.2, S. 28 f.

Systeme und Daten wird durch Redundanz bei der Datenspeicherung erreicht: durch RAID-Systeme, SAN-Speicher und NAS-Fileserver. Katastrophenfällen wie der Zerstörung der Daten und Systeme durch Wasser, Feuer oder andere externe Einflüsse sollte durch automatisierte Sicherung der Daten und die ausgelagerte Speicherung der gesicherten Daten begegnet werden.⁵⁶

3.4 Verschlüsselung

Wie in Ziffer 2.4 festgestellt, sichert die qualifizierte elektronische Signatur zwar die Integrität der Daten und die Authentizität des Absenders auf höchstem Niveau, sie sichert die Daten aber nicht vor dem Zugriff Unberechtigter. Hiervor müssen die Daten wegen der Anforderungen des Datenschutzrechts und der ärztlichen Schweigepflicht des StGB geschützt werden. Dies ist durch eine Verschlüsselung möglich, die die Funktion eines virtuellen Containers entwickelt. Diese Qualität der Verschlüsselung wurde in Ziffer 2.6 wegen der Anforderungen des Datenschutzrechts und der ärztlichen Schweigepflicht für die elektronische Kommunikation mit Gesundheitsdaten als notwendig bewertet. Damit sind die Daten während der Phase der Archivierung nur dem berechtigten ärztlichen Personenkreis zugänglich. Wenn diese Bedingung technisch erfüllt wird, dann ist auch für die Archivierungsphase eine zentrale Stelle nicht notwendig. Wird die Lösung des virtuellen Containers gewählt, so verwaltet das Personal des Archivierungszentrums nicht personenbezogene Daten, sondern virtuelle Container, die die Daten nur für das berechnete ärztliche Personal zugänglich enthalten. Während der Archivierung dürfen die Daten durch das verarbeitende Personal nicht auf bestimmte Patienten bezogen werden können. Auch in diesem Fall ist die Wahl der Technik frei. Wenn durch die Verschlüsselung und die Technik des virtuellen Containers nur das berechnete ärztliche Personal Zugriff auf die Daten hat, dann ist die zentrale Stelle funktionslos und kann auf sie verzichtet werden.

3.5 Beweisrechtliche Konsequenzen für den Arzthaftungsprozess

Im Arzthaftungsprozess muss sich das elektronische Dokument als Beweismittel bewähren. Der Begriff des elektronischen Dokuments ist auch in das Beweisrecht eingeführt. Nach § 371 Abs. 1 S. 2 ZPO gilt der Beweis mit einem elektronischen Dokument als Augenscheinsbeweis und unterliegt damit nach § 286 ZPO der freien Beweiswürdigung. Das entscheidende Kriterium für die Beweisqualität ist die Integrität des Dokuments. Indiz für die Integrität ist

⁵⁶ VOI Dokumenten-Management, Ziffer 5.6.1-Ziffer 5.6.9, S. 371-384.

die Archivierung nach den Grundsätzen der Ordnungsmäßigkeit. Nach § 371a Abs. 1 Satz 1 ZPO finden auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, die Vorschriften über die Beweiskraft privater Urkunden nach § 416 ZPO entsprechend Anwendung. Die Vorschrift erfasst alle in elektronischer Form vorliegenden Erklärungen. Nach § 371a Abs. 1 Satz 2 ZPO gilt eine Beweiserleichterung zugunsten des Empfängers. Dieser soll entsprechend den für den Beweis des ersten Anscheins entwickelten Grundsätzen den Nachweis, dass die Erklärung von dem Signaturschlüssel-Inhaber abgegeben worden ist, schon durch eine Überprüfung der Signatur erbringen können. Für ein elektronisches Dokument, das von einer öffentlichen Behörde erstellt worden ist, finden nach § 371a Abs. 2 ZPO die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt die Echtheitsvermutung des § 437 ZPO entsprechend.⁵⁷

3.6 Beschlagnahmeverbot

Das Beschlagnahmeverbot medizinischer Dokumente nach § 97 StPO, das nur im Strafverfahren gegen den Patienten gilt, ist eine Folge der ärztlichen Schweigepflicht und des damit verbundenen Zeugnisverweigerungsrechts.⁵⁸ Es ist zu klären, ob dieser Beschlagnahmeschutz auch für die eEPA besteht. Die Beschlagnahmebeschränkungen treten nach § 97 Abs. 2 StPO nur ein, wenn sich die Gegenstände im Gewahrsam des Zeugnisverweigerungsberechtigten befinden. Gewahrsam ist die von einem Herrschaftswillen getragene tatsächliche Sachherrschaft. Problematisch ist, ob bei der Weitergabe der Dokumente an einen Dritten eine solche Sachherrschaft besteht. Hierfür wird ein abgeleiteter Gewahrsam als ausreichend angenommen. Dies wird mit dem Vertrauensverhältnis zwischen Schweigepflichtigem und Patient begründet. Die nach § 53 StGB zur Verweigerung berechtigten Vertrauenspersonen nehmen das Geheimnis grundsätzlich als Inhaber eines Berufs entgegen, der Vertrauen erfordert und verspricht. Geben sie das Beweismittel mit oder ohne Wissen des Patienten aus sachlichen Gründen, die auf der Art des Vertrauensverhältnisses beruhen, in die Hände Dritter, so ist es auch dort vor der Beschlagnahme geschützt, sofern der Dritte auch eine Vertrauensperson im Sinne des § 53 StGB ist, aber sogar auch dann, wenn der Dritte keinem der nach § 53 StGB geschützten

⁵⁷ Zum elektronischen Dokument mit qualifizierter elektronischer Signatur als Beweismittel siehe: *Roßnagel/Fischer Dieskau*, NJW 2006, 806 und *Armigardi/Spalka*, K&R 2007, 26 mit der These, dass wegen der Sicherheitslücken qualifizierter elektronischer Signaturen § 371a Abs. 1 Satz 2 ZPO zugunsten des Signaturschlüssel-Inhabers restriktiv auszulegen ist.

⁵⁸ Zur ausschließlichen Geltung des Beschlagnahmeverbots im Strafverfahren gegen den Patienten *Schlund*, in: *Laufs/Uhlenbruck*, Handbuch des Arztrechts, § 76 Rz. 4.

Berufe angehört.⁵⁹ Deshalb ist der vom Zeugnisverweigerungsberechtigten abgeleitete Gewahrsam auch geschützt, wenn die Dokumente einem Provider übermittelt worden sind. Dies gilt vor allem dann, wenn nach dem in Ziffer 3.4 vorgeschlagenen Modell der Verschlüsselung durch den Provider nicht personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Als Alternative zur Verschlüsselung wird für die wissenschaftliche Forschung die vertrauenswürdige Institution eines Datentreuhänders diskutiert, die selbstgenerierte Pseudonyme verwaltet, über Zuordnungsregeln verfügt, diese gegenüber Dritten vertraulich behandelt und nur zu definierten Zwecken aufdecken darf.⁶⁰ Auch in diesem Falle besteht der Gewahrsam des behandelnden Arztes und damit Beschlagnahmeschutz.

3.7 Haftungsrechtliche Risikominimierung der Dokumentation

Während der Dokumentation sind haftungsrechtlich von besonderer Brisanz die Verantwortlichkeit für die Integrität des Inhalts der Dokumente, die Rechte und Pflichten zum Löschen und Ändern der Dokumente und die Qualität der elektronischen Dokumente.

Für die Integrität der Akte in inhaltlicher Hinsicht ist der einstellende Arzt auf Grund des Behandlungsvertrages verantwortlich. Hiervon kann er sich nicht freizeichnen und die Verantwortlichkeit für die inhaltliche Integrität auf einen Dritten verlagern.

Kritisch sind Informationen, die medizinisch nicht integer sind, anderen Informationen widersprechen, ärztliche Behandlungsfehler dokumentieren und falsch sind. Weist eine Dokumentation einen Fehler auf, so ist der Arzt verpflichtet, die Dokumentation zu berichtigen. Unrichtig sind nur Tatsachen, nicht Werturteile. Diagnosen bewerten nur die beim Patienten aufgetretenen Symptome und behaupten nicht eine Tatsache.⁶¹ Nach den Regeln der ordnungsmäßigen Dokumentation kann das Dokument mit dem unrichtigen Inhalt nicht vernichtet werden, sondern muss um eine Kopie mit dem berichtigten Inhalt ergänzt werden.

Das Einstellen von Informationen und Bilddaten muss in einer Qualität erfolgen, welche die Lesbarkeit der Informationen sicherstellt. Nach diesem Kriterium sind zwar höchste Qualitätsstufen nicht erforderlich, aber suboptimale Qualitäten nicht ausreichend, wenn diese

⁵⁹ Schäfer, in: Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 25. Aufl. 2004, § 97 Rn. 32.

⁶⁰ Bizer, in: *Simitis*, BDSG Kommentar, § 3 Rz. 221.

zu einem Informationsverlust in der Situation der Beurteilung und der Befundarbeitsplätze führen.

Das Einsichtsrecht des Patienten in die Krankenunterlagen muss auch im Falle der eEPA möglich sein.⁶² Sind die Voraussetzungen für ein außerprozessuales, vorprozessuales und prozessuales Einsichtsrecht gegeben, so kann dieses Einsichtsrecht durch die Übergabe ausgedruckter Krankenunterlagen realisiert werden.

3.8 Ergebnis

Die Haftungssicherheit der elektronischen Dokumentation ist von Organisation und Technik abhängig. Konkretisiert werden diese Anforderungen durch die GoBS, die GDPdU, den Nestor-Kriterienkatalog und den Code of Practice des VOI. Durch diese Anforderungen entsteht für die Dokumente Integrität und Authentizität. Der für die Gesundheitsdaten notwendige Schutz nach dem Datenschutzrecht und dem Strafrecht wird durch die Technik der Verschlüsselung erreicht. Wenn diese Verschlüsselung die Funktion eines virtuellen Containers hat, sodass für den Provider die Daten nicht erkennbar sind, dann ist die zentrale Stelle verzichtbar. Beweisrechtliche Qualität, die für den Arzthaftungsprozess wichtig ist, entsteht durch die elektronische Dokumentation nach den Grundsätzen der Ordnungsmäßigkeit. Die von einem Provider gespeicherten Dokumente stehen unter Beschlagnahmeschutz, da der einstellende ,Arzt den Gewahrsam an den Dokumenten ausüben kann. Die Minimierung des Haftungsrisikos für die Dokumentation wird bestimmt durch die Integrität der Dokumente, die Berechtigung zur Korrektur falscher Inhalte und die technische Qualität der Dokumentation.

⁶¹ Uhlenbruck/Schlund, in Laufs (Hrsg.), Handbuch des Arztrechts, § 60 Rz.15.

⁶² Zum Einsichtsrecht des Patienten: Uhlenbruck/Schlund, in Laufs (Hrsg.), Handbuch des Arztrechts, § 60 Rz.1-13; Laufs, Arztrecht, Rz. 325-332 und Schirmer, in: Rossnagel, Handbuch des Datenschutzrechts, S. 96.

4.0 Der Provider als Auftragsdatenverarbeiter

Der Provider ist die Stelle, die die technische Durchführung der eEPA übernommen hat. Werden Patientendaten in einem Zentralarchiv eines Dienstleisters gespeichert, so ist dies eine datenschutzrechtlich kritische Situation: Die Verarbeitung der Daten durch einen Dienstleister ist nur im Rahmen eines Auftragsverhältnisses (4.1) unter Beachtung der ärztlichen Schweigepflicht (4.2) möglich. Unter diesen Bedingungen ist im Ergebnis die Institution einer zentralen Stelle funktionslos (4.3).

4.1 Datenverarbeitung im Auftrag

Der Auftraggeber darf nur Hilfsfunktionen, aber nicht Funktionen an den Auftragnehmer vergeben (4.1.1), den er sorgfältig auszuwählen hat (4.1.2). Der Auftrag ist schriftlich zu erteilen (4.1.3). In dem Vertrag ist deutlich zu machen, dass der Auftragnehmer gegenüber dem Auftraggeber weisungsgebunden ist (4.1.4). Damit ist auf der primären Ebene der behandelnden Ärzte mit dem Provider ein Vertrag über die Auftragsdatenverarbeitung abzuschließen (4.1.5).

4.1.1 Datenverarbeitung als Hilfsfunktion

Für die Datenverarbeitung im Auftrag gemäß § 11 BDSG ist die wichtigste Voraussetzung, dass die Erhebung, Verarbeitung und Nutzung lediglich in ihrer Hilfsfunktion für die Erfüllung der Aufgaben und Geschäftszwecke der verantwortlichen Stelle ausgelagert wird. Werden die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecke teilweise abgegeben oder erbringt der externe Datenverarbeiter über die technische Verarbeitung hinaus materielle vertragliche Leistungen mit Hilfe der überlassenen Daten, dann ist er nicht mehr bloßer Auftragnehmer, sondern wird selbst zur verantwortlichen Stelle. Die Datenweitergabe im Rahmen einer solchen „Funktionsübertragung“ ist konsequenterweise als Übermittlung zu klassifizieren.⁶³

4.1.2 Pflichten des Auftraggebers

Der Auftraggeber ist nach § 11 Abs. 2, Satz 1 und 4 BDSG zur sorgfältigen Auswahl des Auftragnehmers verpflichtet. Wichtigster Maßstab für die Auswahl des Auftragnehmers ist

⁶³ Walz, in: *Simitis*, BDSG, § 11 Rdnr. 18

nach § 11 Absatz 2 Satz 1 BDSG die „Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen“. Entscheidendes Kriterium hierfür ist, ob bei der beauftragten Stelle ein angemessener Datensicherungsstandard gewährleistet ist, der den Anforderungen des § 9 BDSG und der Anlage zu dieser Vorschrift entspricht. Dies gilt insbesondere für die in Nr. 6 der Anlage genannte „Auftragskontrolle“, die sicherstellen soll, dass der Auftragnehmer mit den ihm anvertrauten Daten nur entsprechend den Weisungen des Auftraggebers umgeht.⁶⁴

Die Auswahlentscheidung setzt nach § 11 Abs. 2 Satz 4 BDSG voraus, dass der Auftraggeber sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Jedenfalls sollte der Auftraggeber das bei der beauftragten Stelle realisierte Datensicherungskonzept zur Kenntnis nehmen.⁶⁵

Unabdingbare Voraussetzung ist, dass die Mitarbeiter des Auftragnehmers auf das Datengeheimnis nach § 5 BDSG verpflichtet sind.

4.1.3 Auftragserteilung

§ 11 Abs. 2 Satz 2 BDSG verlangt, dass der Auftrag schriftlich zu erteilen ist. In dem schriftlichen Vertrag sind die „Datenerhebung, -verarbeitung oder –nutzung“ festzulegen. Damit sind die Phasen der Datenverarbeitung angesprochen. Zu fixieren sind ferner die „technischen und organisatorischen Maßnahmen“ der Datensicherung. Sie müssen den Zeitraum vom Eingang der Daten beim Auftragnehmer bis zur Ablieferung beim Auftraggeber umfassen.⁶⁶ Schließlich sind „etwaige Unterauftragsverhältnisse“ festzulegen, die durch die Einschaltung von Subunternehmern entstehen. Die Vergabe von Unteraufträgen darf vom Auftraggeber nur gestattet werden, wenn der Auftragnehmer zusichert, dass die ihm obliegenden Pflichten auch vom Unterauftragnehmer eingehalten werden.⁶⁷

4.1.4 Weisungsbindung des Auftragnehmers

Der Auftragnehmer darf nach § 11 Abs. 3 Satz 1 BDSG die Daten nur „im Rahmen der Weisungen des Auftraggebers“ erheben, verarbeiten und nutzen. Unter „Weisungen“ sind alle vom Auftragnehmer vertraglich übernommenen Pflichten in Bezug auf Art und Gegenstand der Erhebung, Verarbeitung oder Nutzung sowie die technisch-organisatorische

⁶⁴ Walz, in: *Simitis*, BDSG, § 11 Rdnr. 42.

⁶⁵ Walz, in: *Simitis*, BDSG, § 11 Rdnr. 45.

⁶⁶ Walz, in: *Simitis*, BDSG, § 11 Rdnr. 50.

⁶⁷ Walz, in: *Simitis*, BDSG, § 11 Rdnr. 51.

Datensicherung zu verstehen. Hinzu kommen die Einzelweisungen im laufenden Auftragsverhältnis. Verboten sind dem Auftragnehmer insbesondere die Weitergabe oder Übermittlung der Daten an Dritte, die Auskunftserteilung an den Betroffenen, die Verwendung für eigene Geschäftszwecke, die Nutzung für andere Auftraggeber sowie die Fortsetzung der Speicherung nach Auftragsabwicklung.⁶⁸ Wesentlicher Bestandteil dieses Vertrages ist, dass der Auftragnehmer die Dokumente nach den in Ziffer 3.0 entwickelten Anforderungen der Ordnungsmäßigkeit dokumentiert, um das Haftungsrisiko der einstellenden Ärzte für ihren Verantwortungsbereich der Dokumentation möglichst zu reduzieren.

4.1.5 Konsequenzen für die primäre Ebene der behandelnden Ärzte

Diese Regeln über die Auftragsdatenverarbeitung ermöglichen es, dass auf der primären Ebene der behandelnden Ärzte mit dem Provider Verträge abgeschlossen werden, in denen die Verarbeitung der medizinischen Dokumente als Hilfsfunktion geregelt, der Provider als Auftragnehmer nach den Kriterien der Eignung ausgesucht, der Auftrag schriftlich erteilt und der Provider an die Weisungen der beauftragenden Ärzte gebunden ist.

4.2 Die Konsequenzen der ärztlichen Schweigepflicht für den Provider

In Ziffer 1.0 ist ausgeführt worden, dass wegen der ärztlichen Schweigepflicht Patientendaten nur von Ärzten und deren Hilfspersonen im Zusammenhang mit dem Behandlungsvertrag verarbeitet werden dürfen.⁶⁹ Dies hat Konsequenzen für die Phase des Transports der Daten durch das Netz und die Phase der Dokumentation. In beiden Fällen müssen die Daten vor dem Zugriff nicht-ärztlichen Personals sicher sein. Eine mögliche technische Lösung ist die Verschlüsselung der Patientendaten. Für den elektronischen Transport ist dies in Ziffer 2.6 und für die elektronische Dokumentation in Ziffer 3.4 ausgeführt worden. Die Verschlüsselung während der Dokumentation bedeutet, dass die Gesundheitsdaten durch den Auftragnehmer nicht eingesehen werden können und damit die Anforderungen der ärztlichen Schweigepflicht erfüllt werden. Nur unter dieser Bedingung ist die Auftragsdatenverarbeitung zulässig. Eine zentrale Stelle, die zwischen die primäre Ebene der behandelnden Ärzte und den Provider eingeschaltet ist, ist unter diesen Umständen funktionslos. Einstellender und abrufender Arzt können, wenn sie auf Grund des Behandlungsvertrages berechtigt sind, direkt auf die Gesundheitsdaten zugreifen. Ihre Rechtsbeziehung zu dem Provider ist jeweils durch einen Vertrag über die Auftragsdatenverarbeitung zu regeln. Wird statt der

⁶⁸ Walz, in: *Simitis*, BDSG, § 11 Rdnr.57.

⁶⁹ Walz, in: *Simitis*, BDSG, § 11Rdnr. 33.

Verschlüsselung die Sicherheitstechnik der Anonymisierung und Pseudonymisierung gewählt, so ist eine zentrale Stelle notwendig, um die Anonymisierungs und Pseudonymisierungslisten zu verwalten, die als Schlüssel dienen, um die Daten den Patienten zuzuordnen. Die Beziehung zwischen zentraler Stelle und Provider muss auch in diesem Falle durch einen Auftragsdatenvertrag geregelt werden.

4.3 Ergebnis

Wesentlicher Bestandteil des Vertrages zwischen einstellenden Ärzten als Auftraggeber und Provider als Auftragnehmer ist, dass der Provider die Dokumente nach den in Ziffer 3.0 entwickelten Anforderungen der Ordnungsmäßigkeit dokumentiert, um das Haftungsrisiko der einstellenden Ärzte für ihren Verantwortungsbereich der Dokumentation möglichst zu reduzieren. In den Vertrag ist die Pflicht zu integrieren, dass der Provider verschlüsselte Daten verwaltet. Damit ist gesichert, dass der Provider die Gesundheitsdaten nicht einsehen kann und wird die ärztliche Schweigepflicht gewahrt. Unter diesen Bedingungen ist eine zentrale Stelle, die zwischen die primäre Ebene der behandelnden Ärzte und den Provider eingeschaltet ist, funktionslos. Einstellender und abrufender Arzt können auf Grund eines solchen Auftragsdatenverhältnisses direkt auf die Daten bei dem Provider zugreifen, wenn sie dazu durch den Behandlungsvertrag berechtigt sind.

5.0 Die Datentreuhänder-Lösung, Datenschutz und Beschlagnahmeschutz

Die Alternative zur Verschlüsselung ist das Konzept der Datentreuhänderschaft (5.1). Mit diesem Konzept sind datenschutzrechtliche Probleme (5.2) und das strafprozessrechtliche Problem des Beschlagnahmeschutzes der Daten bei der datenspeichernden Stelle verbunden (5.3).

5.1 Datentreuhänderschaft

Nach dem Datentreuhänder-Konzept, einem speziell bei epidemiologischen Untersuchungen seit Ende der achtziger Jahre eingesetzten Pseudonymisierungsverfahren, übernimmt ein Datentreuhänder die Rolle einer vertrauenswürdigen Stelle zwischen der datenspeichernden Stelle, der wissenschaftlichen Institution und den Patienten. Der Datentreuhänder pseudonymisiert die Patientendaten und führt den Zusammenhang zwischen identifizierenden Patientendaten und Pseudonymen in einer elektronischen Patientenliste.⁷⁰ Nur der Datentreuhänder verfügt über die Zuordnungsregel zwischen Pseudonym und Person. Er muss diese gegenüber Dritten vertraulich behandeln und darf sie nur zu definierten Zwecken aufdecken. Hierzu ist der Datentreuhänder durch Vertrag gegenüber der betroffenen Person und der wissenschaftlichen Institution verpflichtet.

5.2 Datenschutzrechtliche Probleme

Komplexe Datenbestände führen zu einer datenschutzrechtlich problematischen Situation: Durch das Zusammenführen von Daten unter Nutzung des Personenbezugs können Persönlichkeitsprofile hergestellt werden.⁷¹ Dies ist im Falle von Gesundheitsdaten von besonderer Brisanz. Als Datenschutzkonzept in dieser Risikosituation gilt die aus dem informationellen Selbstbestimmungsrecht abgeleitete informationelle Gewaltenteilung (5.2.1). Die Einwilligung des Betroffenen ist hierfür nicht erforderlich, wenn die informationelle Gewaltenteilung für ihn nicht zu einem Rechtsverlust führt (5.2.2). Hierfür ist entscheidend, dass der Betroffene gegenüber komplexen Datenbeständen sein Recht auf Auskunft und damit seine Rechte auf Sperrung, Berichtigung, Löschung und Schadensersatz geltend machen kann (5.2.3).

⁷⁰ Zum Verfahren der Pseudonymisierung siehe *Bizer*, in *Simitis*, BDSG, § 3 Rz. 219-222.

⁷¹ Ziffer 6.1.3 des 3. Tätigkeitsberichts des Landesbeauftragten für den Datenschutz des Landes Brandenburg <http://www.lida.brandenburg.de>.

5.2.1 Informationelle Gewaltenteilung

Der Rechtsgedanke der informationellen Gewaltenteilung ist durch die „Telematikplattform für medizinische Forschungsnetze e.V.“ in die Diskussion um die datenschutzrechtliche Sicherheit gespeicherter Patientendaten eingeführt worden.⁷² Dieser Rechtsgedanke findet seine Grundlage in dem informationellen Selbstbestimmungsrecht. Personenbezogene Daten werden nach dem Volkszählungsurteil des Bundesverfassungsgerichts durch das Recht auf informationelle Selbstbestimmung verfassungsrechtlich geschützt: die Befugnis, über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen.⁷³ Das Bundesverfassungsgericht verdeutlicht im Volkszählungsurteil, dass es das informationelle Selbstbestimmungsrecht nicht in einer sphärenbezogenen Weise interpretiert, sondern dass dieses Recht vor Gefahren schützt, die sich aus der Zusammenfügung mit anderen Datensammlungen zu einem mehr oder weniger vollständigen Persönlichkeitsbild ergeben, dessen Richtigkeit und Verwendung der Betroffene nur unzureichend kontrollieren kann.⁷⁴ Damit entfaltet das Recht auf informationelle Selbstbestimmung einen flexiblen, gegenüber technischen und gesellschaftlichen Entwicklungen reagiblen und an der konkreten Gefährdungssituation ausgerichteten Gewährleistungsgehalt.⁷⁵ Gemessen an dieser Anforderung des informationellen Selbstbestimmungsrechts ist der organisatorische Aufwand der Datentreuhänderschaft unumgänglich, denn schlichte Pseudonymisierungstechniken wie das von dem Betroffenen oder der datenverarbeitenden Stelle ausgewählte und verwaltete Pseudonym entsprechen nicht dem Prinzip der informationellen Gewaltenteilung. Im Falle des von dem Betroffenen selbstgenerierten Pseudonyms liegt die Sicherheit der Zuordnungsregel allein in der Hand des Namensträgers. Wird das Pseudonym, wie im Falle von Internetportalen, von der datenspeichernden Stelle vergeben und verwaltet, so schützt das Pseudonym zwar gegenüber Dritten, nicht aber gegenüber der datenspeichernden Stelle. Als Pseudonymisierungstechnik für Gesundheitsdaten kommt damit nur die Datentreuhänderschaft in Frage, die das Prinzip der informationellen Gewaltenteilung möglichst anspruchsvoll umsetzt. Die Datentreuhänderschaft, auf die Situation der eEPA angewandt, bedeutet, dass ein Datentreuhänder Patientendaten mit den dazugehörigen Inhalten von einem einstellenden Arzt erhält und pseudonymisiert, indem er die Inhalte mit Pseudonymen an eine datenspeichernde Stelle übermittelt.

⁷² <http://www.tmf-ev.de>.

⁷³ BVerfGE 65, 1 (41 ff.); siehe zum informationellen Selbstbestimmungsrecht *Gola/Schomerus*, § 1 Rz. 6, 11 und *Trute*, in: *Rossnagel* (Hrsg.) Handbuch Datenschutzrecht, 2.5 Verfassungsrechtliche Grundlagen, S. 156-187.

⁷⁴ BVerfGE 65, 1 (42).

⁷⁵ Auf die Gefährdungsabhängigkeit stellt *Trute*, in: *Rossnagel* (Hrsg.), Handbuch des Datenschutzrechts,

5.2.2 Datentreuhänderschaft und das Problem der Einwilligung

Das Problem der Einwilligung im Zusammenhang mit der Datentreuhänderschaft ist anlässlich des Projektes „Quasi-Niere“ diskutiert worden. In der Praxis ist eine Form der Datentreuhänderschaft aufgebaut worden, um das Projekt „Quasi-Niere“ zu realisieren, das die Qualität von Nierenersatztherapien sichern soll. Die einzelnen Behandlungseinrichtungen (Dialysezentren) liefern patientenbezogene Daten mittels eines Formblatts an einen „Datentreuhänder“. Dieser pseudonymisiert die Behandlungsdaten, sodass sie durch niemanden außer der Vertrauensstelle als Datentreuhänder einem Patienten zugeordnet werden können. Behandlungsdaten werden nicht in der Vertrauensstelle gespeichert, sondern bei Quasi-Niere, wo diese ohne Personenbezug archiviert und analysiert werden. Ein Patient oder ein behandelnder Arzt kann seine gespeicherten Behandlungsdaten bei der Vertrauensstelle anfordern. Nachdem die Vertrauensstelle die Anfrage überprüft hat, werden die Behandlungsdaten von Quasi-Niere über die Vertrauensstelle vertrauenswürdig an den Patienten oder den behandelnden Arzt übermittelt.⁷⁶ Als Problem wurde diskutiert, ob es einer Einwilligung des Betroffenen bedarf. Dies sollte nicht notwendig sein, da nach § 137 SGB V Krankenhäuser verpflichtet sind, sich an Maßnahmen der Qualitätssicherung zu beteiligen. Der Bayerische Landesdatenschutz-beauftragte hielt dagegen eine Einwilligung des Betroffenen für erforderlich.⁷⁷ Das Problem wurde in Zusammenarbeit mit dem Berliner Datenschutzbeauftragten auf der Grundlage von § 299 SGB V gelöst, wonach eine Verarbeitung von pseudonymisierten Daten ohne eine Einwilligung des Patienten möglich ist. Entsprechend speichert Quasi-Niere die von einem Notar pseudonymisierten Patientendaten ohne Einwilligung des Patienten. Diese Lösung ist mit dem europäischen Datenschutzpreis e-PRODAT ausgezeichnet worden.⁷⁸ Die verfassungsrechtliche Argumentation für die Verarbeitung von Patientendaten ohne Einwilligung des Patienten ergibt sich aus dem Aspekt der informationellen Gewaltenteilung: Wird durch die informationelle Gewaltenteilung der Eingriff in das Recht auf informationelle Selbstbestimmung vermieden, so ist weder eine Einwilligung noch eine gesetzliche Erlaubnis erforderlich, denn es entsteht kein Rechtsnachteil zu Lasten des Betroffenen, der eine gesetzliche Erlaubnis oder eine

2.5 Verfassungsrechtliche Grundlagen, S. 156 ff., Rn. 14, ab.

⁷⁶ <http://www.quasi-niere.de/faq>.

⁷⁷ Der Bayerische Landesbeauftragte für den Datenschutz, 17. Tätigkeitsbericht, 1996, Ziffer 3.3.2. „Quasi-Niere“.

⁷⁸ www.quasi-niere.de/datenschutzpreis (Stand: 10.5.2008).

Einwilligung notwendig machen würde. Diese Argumentation ist nur akzeptabel, wenn der Betroffene sein Auskunftsrecht und damit seine Betroffenenrechte geltend machen kann.

5.2.3 Auskunftsanspruch

Der Auskunftsanspruch ist der Schlüssel zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung, denn nur wenn der Auskunftsanspruch realisiert werden kann, können die Betroffenenrechte wie Sperrung, Berichtigung, Löschung, Widerspruch und Schadensersatz durchgesetzt werden. In komplexen und stellenübergreifenden Datenflüssen wie in der medizinischen Datenverarbeitung wird die Realisierung des Auskunftsanspruchs kritisch. In der Telematik-Infrastruktur werden Behandlungs-, Dokumentations-, Abrechnungs- und Forschungszwecke verfolgt, an denen datenerhebende Ärzte, weiter behandelnde und konsultierte Ärzte, Krankenhäuser, Krankenkassen und Kompetenzzentren beteiligt sind. Die Arbeitsteilung kann sich auf Erhebung, Übermittlung, Speicherung, Administration, Pseudonymisierung, Auswertung beziehen. Bei einer derartigen stellenübergreifenden Datenverarbeitung besteht für den Betroffenen die Gefahr, dass er die Stelle nicht feststellen kann, gegen die er den Auskunftsanspruch geltend machen kann. Damit muss der Betroffene die Kette der Datenverarbeiter mit Auskunftsanträgen durchlaufen. Erst nach Kenntnis von Empfängern und Absendern kann er an diese das Auskunftersuchen stellen. Dieses Problem des Auskunftsanspruchs in der Situation kombinierter Datenverarbeitung hat der Gesetzgeber für Verbunddateien (§ 6 Abs. 2 BDSG) und Chipkarten (§ 6c BDSG) geregelt. Im Falle der Verbunddateien ist der Betroffene berechtigt, sich an jede Stelle zu wenden, wenn er nicht feststellen kann, welche Stelle die Daten gespeichert hat. Im Falle der Chipkarten hat die Stelle, die Chipkarten ausgibt, den Betroffenen über ihre Identität zu informieren. In komplexen und arbeitsteiligen Verfahren können nach dem Vorbild der „automatisierten Entscheidungen“ in § 6a Abs. 3 BDSG, wonach sich die Auskunft auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten erstreckt, allgemeine Systeminformationen von Bedeutung sein. Die Auskunft sollte sämtliche relevanten Auswertungen und Interpretationen, die den verarbeitenden Stellen zur Verfügung stehen, umfassen. In diesem Zusammenhang stellen sich Fragen, zu welchem Zweck und in welcher Form an welche Person Daten weitergegeben werden und wie durch einen verteilten Datenfluss der Datenschutz am effektivsten realisiert werden kann. Verfügt die verarbeitende Stelle über Verknüpfungsmöglichkeiten mit weiteren abstrakten oder anderweitigen persönlichen Informationen, die die Interpretation der individuellen Daten ermöglicht, so ist diese Interpretation auch dem Betroffenen anzubieten. Diese Grundsätze sind auf den Auskunftsanspruch im Zusammenhang mit der eEPA anwendbar. Nach dem Vorbild der

Verbunddateien (§ 6 Abs. 2 BDSG) wird eine Stelle benannt, an die sich der Betroffene wenden kann. Hierfür bietet sich die Datentreuhänderstelle an.⁷⁹ Über deren Identität ist der Betroffene nach dem Vorbild der Regelung für Chipkarten (§ 6c BDSG) zu informieren. Die Auskunft umfasst nach dem Vorbild der automatisierten Entscheidung (§ 6a Abs. 3 BDSG) auch allgemeine Systeminformationen.

5.3 Beschlagnahmeschutz

Wie unter Ziffer 3.6 „Beschlagnahmeverbot“ ausgeführt, tritt der Beschlagnahmeschutz nach § 97 Abs. 2 Satz 1 StPO ein, wenn sich die Gegenstände im Gewahrsam der Zeugnisverweigerungsberechtigten befinden, wobei Gewahrsam die tatsächliche Sachherrschaft ist. Die tatsächliche Sachherrschaft wird als fortbestehend angenommen, wenn die Zeugnisverweigerungsberechtigten die Beweismittel aus sachlichen Gründen, die auf der Art des Vertrauensverhältnisses beruhen, Dritten übergeben, die keinem der nach § 53 StGB geschützten Berufe angehören.⁸⁰ Unter Ziffer 3.6 wurde festgestellt, dass der Gewahrsam des einstellenden Arztes und damit der Beschlagnahmeschutz besteht, wenn die Dokumente verschlüsselt der datenspeichernden Stelle übergeben werden. Der Beschlagnahmeschutz besteht nach der Gesetzeslage selbst über diese Situation der Speicherung verschlüsselter Daten durch einen Dienstleister hinaus: Nach § 97 Abs. 2 Satz 2 StPO besteht der Beschlagnahmeschutz für Gegenstände im Gewahrsam eines Dienstleisters, der für zeugnisverweigerungsberechtigte Ärzte personenbezogene Daten erhebt, verarbeitet oder nutzt.⁸¹ Ist der Gewahrsam und damit der Beschlagnahmeschutz gegeben, wenn der Dritte für den zeugnisverweigerungsberechtigten Arzt personenbezogene Daten verarbeitet, so kann angenommen werden, dass der Gewahrsam und damit der Beschlagnahmeschutz auch besteht, wenn durch informationelle Gewaltenteilung der Datenschutz für die Patientendaten realisiert wird, indem die datenspeichernde Stelle die von einem Datentreuhänder pseudonymisierten Dokumente erhält.⁸² Wenn die Datentreuhänderschaft der eEPA in dieser Form organisiert wird, dann ist auch Beschlagnahmeschutz gegeben.

⁷⁹ Weichert, Datenschutz-Auskunftserteilung in verteilten Systemen, <http://www.datenschutzzentrum.de/vortraege/061006>.

⁸⁰ Schäfer in Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 25. Aufl. 2004, § 97 Rz. 32.

⁸¹ Siehe hierzu Meyer-Goßner, Strafprozessordnung, 47. Aufl., § 97 Rz. 14 und Schäfer, in: Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Zweiter Band, 25. Aufl., § 97 Rz. 118.

⁸² Zu diesem Ergebnis kommt auch Dierks in seinem bisher unveröffentlichten Gutachten für die „Telematikplattform für medizinische Forschungsnetze e.V.“ wie unter <http://www.tmf-ev.de> mitgeteilt.

5.4 Ergebnis

- **Datentreuhänderschaft und Pseudonymisierung**

Als Alternative zur Verschlüsselungstechnik kommt für die Speicherung von Gesundheitsdaten die Pseudonymisierung durch Datentreuhänderschaft in Frage. Die Datentreuhänderschaft, auf die Situation der eEPA angewandt, bedeutet, dass der Datentreuhänder Patientendaten mit den dazugehörigen Inhalten von dem einstellenden Arzt erhält und pseudonymisiert, hierüber eine elektronische Patientenliste führt und die pseudonymisierten Inhalte an die datenspeichernde Stelle übermittelt.

- **Datenschutz**

Wird durch die informationelle Gewaltenteilung der Grundrechtseingriff vermieden, so ist eine Einwilligung nicht erforderlich. Dies bedingt, dass kein Rechtsverlust besteht, also das Auskunftsrecht und die übrigen Betroffenenrechte realisierbar sind. Dem Betroffenen wird eine Stelle benannt, an die er sich wenden kann, um seinen Auskunftsanspruch und die anderen Betroffenenrechte geltend zu machen. Hierfür bietet sich die Datentreuhänderstelle an.⁸³ Die Auskunft umfasst nach dem Vorbild der automatisierten Entscheidung (§ 6a Abs. 3 BDSG) auch allgemeine Systeminformationen.

- **Beschlagnahmeschutz**

Der Beschlagnahmeschutz besteht auch, wenn durch informationelle Gewaltenteilung der Datenschutz für die Patientendaten realisiert wird, indem die datenspeichernde Stelle die von einem Datentreuhänder pseudonymisierten Dokumente erhält.⁸⁴ Wenn die Datentreuhänderschaft der eEPA in dieser Form organisiert wird, dann ist auch Beschlagnahmeschutz gegeben.

⁸³ Weichert, Datenschutz-Auskunftserteilung in verteilten Systemen, <http://www.datenschutzzentrum.de/vortraege/061006>

⁸⁴ Zu diesem Ergebnis kommt auch Dierks in seinem bisher unveröffentlichten Gutachten für die „Telematikplattform für medizinische Forschungsnetze e.V.“ wie unter <http://www.tmf-ev.de> mitgeteilt.

6.0 Haftungsrisiken des einstellenden und des abrufenden Arztes

Die Rechte und Pflichten des einstellenden Arztes (6.1) und des abrufenden Arztes (6.2) stehen in einem wechselseitigen Verhältnis.

6.1 Einstellender Arzt

Werden Dokumente ohne einen konkreten und bekannten Adressaten in die eEPA eingestellt, dann ist der Zusammenhang, in dem die Inhalte dieser Dokumente in Zukunft genutzt werden, nicht absehbar. Dies ist nicht das Rechtsrisiko des einstellenden Arztes. Der einstellende Arzt hat seine Pflichten erfüllt, wenn er die Dokumente im Falle der Verschlüsselungslösung dem nach § 11 BDSG als Auftragsdatenverarbeiter ausgewählten Provider oder im Falle der Datentreuhänderlösung dem Datentreuhänder übergeben hat. Diese Rechtslage kann der einstellende Arzt gegenüber dem abrufenden Arzt durch eine "Freizeichnung" deutlich machen, in der seine Verantwortung und deren Grenzen aufgezeigt werden.⁸⁵ Der einstellende Arzt ist für die Einstellung der Dokumente in die eEPA verantwortlich. Im Rahmen dieser Verantwortlichkeit ist folgendes geregelt:

- Der einstellende Arzt kann den Zugriff zeitlich beschränken, wenn dies sachlich berechtigt ist und durch diese Beschränkung und eine damit fehlende Information die mögliche Heilbehandlung nicht gefährdet wird.
- Der einstellende Arzt kann auch bestimmen, wenn dies nach dem Behandlungsvertrag gerechtfertigt ist, dass nicht alle Informationen, sondern nur die behandlungsrelevanten Informationen in die eEPA eingestellt werden.
- Erhält ein Arzt im Rahmen eines Behandlungsvertrages von einem anderen Arzt eine Behandlungsinformation, so ist er berechtigt, diese in die eEPA einzustellen, um damit seine Dokumentationspflichten im Rahmen der Behandlung zu erfüllen.

Der einstellende Arzt sollte durch Nutzungsbedingungen der eEPA darauf hingewiesen werden, dass er die Möglichkeit der Freizeichnung hat.

6.2 Abrufender Arzt

Durch die Freizeichnung des einstellenden Arztes geht das Rechtsrisiko auf den Arzt über, der die Dokumente abrufen. Der Abruf erfolgt im Falle der Verschlüsselungslösung von dem Provider und im Falle der Datentreuhänderlösung von dem Datentreuhänder. Der abrufende Arzt muss verantworten, dass der Abruf im Rahmen des Behandlungsvertrages notwendig

⁸⁵ Zur Freizeichnung aus dem Gesichtspunkt der Risikobeherrschung *Basedow* in *Krüger*, Münchener Kommentar zum Bürgerlichen Gesetzbuch Band 2a, 4. Aufl., 2003, § 307 Rz. 44-45.

und damit datenschutzrechtlich zulässig ist. Wie die Rechte und Pflichten des einstellenden Arztes, so werden auch die Rechte und Pflichten des abrufenden Arztes durch den Zweck des Behandlungsvertrages bestimmt. Dies verpflichtet ihn, die für die Behandlung notwendigen Informationen zu nutzen. Hierzu gehört auch die Nutzung der eEPA. Diese Nutzung ist sozialadäquat und weder organisatorisch noch wirtschaftlich unangemessen. Danach würde der behandelnde Arzt den Behandlungsvertrag verletzen und gegenüber dem Patienten für einen hierdurch verursachten Schaden haften, wenn er die eEPA nicht nutzen, relevante Informationen aus der eEPA nicht würdigen oder die aus der eEPA erreichbaren und für die Behandlung notwendigen Informationen nur partiell abrufen würde.

6.3 Ergebnis

Durch Nutzungsbedingungen für die eEPA sollte für den einstellenden Arzt die Möglichkeit der „Freizeichnung“ bestimmt werden, mit der er auf die Einstellung der Dokumente entsprechend dem Zweck des Behandlungsvertrages und auf die Grenzen der Freizeichnung für vorsätzliches und grob fahrlässiges Verschulden hingewiesen wird. Für den abrufenden Arzt sollte klargestellt werden, dass er zum Abruf und zur Verwertung der Dokumente entsprechend dem Zweck des Behandlungsvertrages verpflichtet ist.

7.0 Die elektronische Gesundheitskarte in der gesetzlichen Krankenversicherung

Für die gesetzliche Krankenversicherung ist die eEPA nicht gesetzlich geregelt. Damit gelten die allgemeinen Grundsätze, wie sie vorstehend entwickelt worden sind, soweit sich nicht spezielle Rechtsaspekte aus dem Sozialversicherungsrecht ergeben. Es liegt nahe, hierfür die Vorschrift zur elektronischen Gesundheitskarte (§ 291a SGB V) als ein der eEPA vergleichbares Modell elektronischer Kommunikation und Dokumentation zu berücksichtigen. Die elektronische Gesundheitskarte ist nach § 291a Abs. 1 SGB V die Erweiterung der Krankenversichertenkarte nach § 291 Abs. 1 SGB V. Nach § 291a Abs. 1a SGB V sind die Vorschriften auf die privaten Krankenversicherungen entsprechend anzuwenden. Die elektronische Gesundheitskarte muss nach § 291a Abs. 2 SGB V die Angaben nach § 291 Abs. 2 SGB V und die Angaben nach § 291a Abs. 2 SGB V für die Übermittlung ärztlicher Verordnungen (Nr. 1) und den Berechtigungsnachweis zur Inanspruchnahme von Leistungen (Nr. 2) enthalten. Sie muss nach § 291a Abs. 3 Satz 1 SGB V auch geeignet sein, den elektronischen Arztbrief (Nr. 2) und die elektronische Patientenakte (Nr. 4) zu unterstützen (7.1). Der Versicherte muss über die Funktionsweise der Gesundheitskarte informiert werden und seine Einwilligung erteilen, dass mit dem Erheben, Verarbeiten und Nutzen seiner Daten begonnen werden kann (7.2). Zugriffsberechtigt auf die Daten mittels der elektronischen Gesundheitskarte sind Ärzte und Apotheker und die Versicherten (7.3). Für die Versicherten ist ein Recht auf Löschung der Daten vorgesehen (7.4). Im Ergebnis sind die elektronische Gesundheitskarte und eine fall- und einrichtungsübergreifende elektronische Patientenakte Bestandteile eines Systems (7.5).

7.1 Angaben und Anwendungen der elektronischen Gesundheitskarte

Die elektronische Gesundheitskarte muss nach § 291a Abs. 2 SGB V Angaben nach § 291 Abs. 2 SGB V enthalten und geeignet sein, Angaben für die Übermittlung ärztlicher Verordnungen und den Berechtigungsnachweis zur Inanspruchnahme von Leistungen aufzunehmen. Nach § 291a Abs. 3 Satz 1 SGB V muss die elektronische Gesundheitskarte über § 291a Absatz 2 SGB V hinaus neben anderen Anwendungen den elektronischen Arztbrief und eine elektronische Patientenakte - eine fall- und einrichtungsübergreifende Dokumentation über den Patienten - unterstützen. Die Vorschrift setzt somit eine elektronische Patientenakte voraus und bestätigt deren rechtliche Zulässigkeit. Die Inhalte des elektronischen Arztbriefs und der elektronischen Patientenakte sind identisch: Befunde, Diagnosen, Therapieempfehlungen im Falle des elektronischen Arztbriefes, Therapiemaßnahmen im Falle der elektronischen Patientenakte, Behandlungsberichte.

7.2 Die informierte Einwilligung der Versicherten

Nach § 291a Abs. 3 Satz 2 SGB V hat die Krankenkasse spätestens bei Versendung der Karte die Versicherten über deren Funktionsweise einschließlich der Art der auf ihr oder durch sie zu erhebenden, zu verarbeitenden oder zu nutzenden personenbezogenen Daten zu informieren. Die Krankenkasse hat als Stelle, die mobile personenbezogene Speicher- und Verarbeitungsmedien ausgibt, über Identität und Anschrift, Funktionsweise, Rechte des Betroffenen, und zu treffende Maßnahmen bei Verlust oder Zerstörung des Mediums zu informieren, § 291a Abs. 3 Satz 5 SGB V i.V.m. § 6c BDSG. Diese Aufklärungspflicht dient der Transparenz der Kartenstruktur und der auf ihr ablaufenden Datenverarbeitungsprozesse.

⁸⁶ Nach § 291a Abs. 3 Satz 3 SGB V darf mit dem Erheben, Verarbeiten und Nutzen der Daten der Versicherten erst begonnen werden, wenn dazu die Versicherten jeweils gegenüber dem Arzt, Zahnarzt, Psychotherapeuten oder Apotheker ihre Einwilligung erklärt haben. Die Einwilligung bedarf nach § 4a Abs. 1 Satz 3 BDSG der Schriftform. Sie ist nach § 291a Abs. 3 Satz 4, 1. Halbsatz SGB V zu dokumentieren, nach § 291a Abs. 3 Satz 4, 2. Halbsatz SGB V jederzeit widerruflich und kann auf einzelne Anwendungen beschränkt werden.

7.3 Zugriff der Angehörigen eines Heilberufs

Angehörige eines Heilberufs dürfen mittels der elektronischen Gesundheitskarte auf Daten zum Zweck des Erhebens, Verarbeitens oder Nutzens zugreifen, soweit es zur Versorgung der Versicherten erforderlich ist, § 291a Abs. 4 Satz 1 SGB V.

Der Inhalt des Zugriffsrechts wird durch die angegebenen Zwecke des Erhebens, Verarbeitens und Nutzens bestimmt. Dies umfasst den lesenden wie den schreibenden Zugriff und das Recht, die gelesenen Dokumente zu kopieren. Eine Änderung der Dokumente ist nicht möglich, da dadurch eine abgegebene Erklärung verändert würde. Nach den Grundsätzen der ordnungsmäßigen Archivierung muss das Dokument bestehen bleiben und muss die Änderung in einer Kopie des Dokuments erfasst und dokumentiert werden.⁸⁷ Der Urheber kann einer anderen Person, dem Provider oder einer zentralen Stelle, das Recht zur Änderung aus sachlichen Gründen im Einzelfall oder im allgemeinen einräumen.

⁸⁶ Hierzu *Hornung*, Die digitale Identität, S. 60.

⁸⁷ GoBS, Tz. VIII, BStBl. I 1995, S. 7387, 740.

In der Bestimmung, dass auf die Daten zugegriffen werden kann „soweit es zur Versorgung der Versicherten erforderlich ist“, liegt ein grundsätzlicher Systemwechsel des Informationsflusses im Gesundheitswesen. Bislang entschied der Versicherte darüber, welche Leistungserbringer welche Daten erhalten. Das Kriterium der Erforderlichkeit hat dagegen objektiven Charakter, zum Beispiel das aktuelle Krankheitsbild und eventuelle Vorerkrankungen. In manchen Fällen lässt sich objektiv ausschließen, dass bestimmte Daten für bestimmte Berufsgruppen zur Versorgung des Versicherten zur Verfügung stehen müssen. So müssen Apotheker zur Erfüllung ihrer Funktionen nicht notwendig Informationen über Krankheitsdiagnosen oder die gesamte Krankengeschichte erhalten. Deshalb dürfen Apotheker nur auf die diejenigen Daten der Gesundheitskarte zugreifen, die die ärztliche Versorgung betreffen.⁸⁸

Jedes Erheben, Verarbeiten und Nutzen von Daten der freiwilligen Funktionen des § 291a Absatz 3 Satz 1 SGB V mittels der elektronischen Gesundheitskarte ist nach § 291a Abs. 5 Satz 1 SGB V an das Einverständnis des Versicherten gebunden. Das betrifft den lesenden und den schreibenden Zugriff. § 291a Abs. 5 Satz 2 SGB V verlangt (mit Ausnahme der Notfalldaten) eine technische Absicherung der Autorisierung des Versicherten. Dies kann z.B. mittels PIN oder biometrischen Merkmals erfolgen.⁸⁹ Nach § 291a Abs. 5 Satz 3 1. Halbsatz SGB V ist der Zugriff auf die Daten des elektronischen Rezepts und der freiwilligen Funktionen nach § 291a Abs.2 Satz 1 SGB V in jedem Einzelfall an den Einsatz eines elektronischen Heilberufsausweises gebunden, der über die Möglichkeit einer sicheren Authentifizierung und eine qualifizierte elektronische Signatur verfügen muss.

Durch technische Vorkehrungen ist nach § 291a Abs. 6 Satz 2-4 SGB V zu gewährleisten, dass mindestens die letzten 50 Zugriffe auf die Daten protokolliert werden. Die Protokollierung dient dem Zweck der Datenschutzkontrolle. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig.

7.4 Rechte der Versicherten

Die Versicherten haben nach § 291 Abs. 4 Satz 2 SGB V das Recht, auf die Daten nach Abs. 2 Satz 1 und Absatz 3 Satz 1 zuzugreifen. Hierzu gehören nach Abs. 2 Satz 1 die Übermittlung ärztlicher Verordnungen, der elektronische Arztbrief (Abs. 3 Satz 1 Nr. 2) und

⁸⁸ So *Hornung*, Die digitale Identität, S. 224.

⁸⁹ So *Hornung*, Die digitale Identität, S. 63.

die elektronische Patientenakte (Abs. 3 Satz 1 Nr. 4). Hinter diesem missverständlichen Wortlaut verbirgt sich lediglich ein datenschutzrechtliches Auskunftsrecht.⁹⁰

Auf Verlangen des Versicherten müssen die Daten des elektronischen Rezepts wie die der freiwilligen Anwendungen nach § 291a Abs. 3 Satz 1 SGB V gemäß § 291a Abs. 6 Satz 1 SGB V gelöscht werden. Es ist fraglich, ob dieses Recht auf Löschung ohne Einschränkung gilt. Nach dem Wortlaut ist ein Lösungsverlangen nicht an einen Widerruf der Einwilligung gebunden. Danach kann der Versicherte verlangen, dass die Daten einer bestimmten Anwendung gelöscht werden. Ein Problem entsteht, wenn die Anwendung auf eine fortlaufende und vollständige Datenspeicherung angewiesen ist. Wird die Anwendung nach Löschung der bisher erhobenen Daten nicht mehr möglich, so muss in dem Verlangen auf Löschung zugleich ein Widerruf der Einwilligung gesehen werden.⁹¹

Die verantwortliche Stelle, die zur Löschung aufgefordert wird, ist verpflichtet, die Löschung durchzuführen. Dies folgt aus dem Wort „müssen“ im Gesetzestext. Aus Gründen der Nachweisbarkeit muss der Lösungsvorgang von der verantwortlichen Stelle dokumentiert werden. An die Stelle der Löschung tritt nach § 35 Abs. 3 Nr. 1 BDSG die Sperrung, wenn die Daten für eigene Zwecke verarbeitet werden und einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Diese Aufbewahrungspflicht ergibt sich aus der ärztlichen Dokumentationspflicht und dem ärztlichen Haftungsrecht mit der 30-jährigen Verjährungsfrist.

7.5 Ergebnis

Nach den Regeln des § 291a SGB V sind elektronische Gesundheitskarte und elektronische Patientenakte Bestandteile eines Systems, das schlagwortartig als Telemedizin bezeichnet wird. In diesem System hat die elektronische Gesundheitskarte die elektronische Patientenakte zu unterstützen (6.1). Grundlage für dieses System ist das Einverständnis des Versicherten mit dem Zugriff eines Vertreters der Heilberufe auf die elektronische Patientenakte. Danach

- ist die Einwilligung des Versicherten für die erstmalige Verwendung der elektronischen Gesundheitskarte notwendig, um Daten des Versicherten zu erheben, zu verarbeiten und zu nutzen (6.2),

⁹⁰ So *Hornung*, Die digitale Identität, S. 63.

⁹¹ So *Hornung*, Die digitale Identität, S. 64.

- ist für den auf die elektronische Patientenakte zugreifenden Arzt das Einverständnis und die Autorisierung des Versicherten und der elektronische Heilberufsausweis notwendig (6.3),
- sind auf Verlangen des Versicherten die Daten zu löschen (6.4).

Als Ergebnis bedeutet dies für die eEPA, dass § 291a SGB V die eEPA rechtlich nicht in Frage stellt und die eEPA damit rechtlich zulässig ist.

8.0 Ergebnis

8.1 Die zentrale Stelle und das Datenschutzrecht

Der Rahmen der Datenverarbeitung von Gesundheitsdaten wird durch den Behandlungsvertrag bestimmt. Geht die Datenverarbeitung über diesen Zweck hinaus, so ist die Einwilligung des Patienten erforderlich. Werden die Daten gespeichert, um die Dokumentationspflicht zu erfüllen, so begründet dies das Recht zur Speicherung, ohne dass die Einwilligung des Patienten hierfür erforderlich ist. Aus der ärztlichen Schweigepflicht des Strafrechts ergibt sich die Anforderung, dass die Gesundheitsdaten während des elektronischen Transports und der elektronischen Dokumentation vor dem Zugriff nicht-ärztlichen Personals sicher sein müssen. Diese Anforderung kann durch die Verschlüsselungstechnik realisiert werden.

8.2 Haftungssicherheit der elektronischen Kommunikation

Rechtssicherheit und damit Haftungssicherheit für die Kommunikation mit Gesundheitsdaten entsteht durch Integrität des Dokuments und durch Authentizität des Absenders. Diese Funktionen sichern qualifizierte elektronische Signaturen auf hohem Niveau. Durch Verschlüsselungen wird die ärztliche Schweigepflicht gewahrt und der Datenschutz für Gesundheitsdaten erfüllt, da der Inhalt des elektronischen Dokuments vor dem Zugriff Unberechtigter gesichert ist. Diese Anforderungen werden durch die elektronische Gesundheitskarte erfüllt, die aktuell realisiert werden soll. Die Karte erlaubt den Zugriff auf Gesundheitsdaten, die auf anderen Datenspeichern, wie der eEPA, dokumentiert sind. Hierdurch ist eine strategische Allianz zwischen der elektronischen Gesundheitskarte und der eEPA begründet.

8.3 Haftungssicherheit der elektronischen Dokumentation

Die Haftungssicherheit der elektronischen Dokumentation ist von Organisation und Technik abhängig. Konkretisiert werden diese Anforderungen durch die GoBS, die GDPdU, den Nestor-Kriterienkatalog und den Code of Practice des VOI. Durch diese Anforderungen entsteht für die Dokumente Integrität und Authentizität. Der für die Gesundheitsdaten notwendige Schutz nach dem Datenschutzrecht und dem Strafrecht wird durch die Technik der Verschlüsselung erreicht. Wenn diese Verschlüsselung die Funktion eines virtuellen Containers hat, sodass für den Provider die Daten nicht erkennbar sind, dann ist die zentrale Stelle verzichtbar. Beweisrechtliche Qualität, die für den Arzthaftungsprozess wichtig ist,

entsteht durch die elektronische Dokumentation nach den Grundsätzen der Ordnungsmäßigkeit. Die von einem Provider gespeicherten Dokumente stehen unter Beschlagnahmeschutz, da der einstellende ,Arzt den Gewahrsam an den Dokumenten ausüben kann. Die Minimierung des Haftungsrisikos für die Dokumentation wird bestimmt durch die Integrität der Dokumente, die Berechtigung zur Korrektur falscher Inhalte und die technische Qualität der Dokumentation.

8.4 Der Provider als Auftragsdatenverarbeiter

Wesentlicher Bestandteil des Vertrages zwischen einstellenden Ärzten als Auftraggeber und Provider als Auftragnehmer ist, dass der Provider die Dokumente nach den in Ziffer 3.0 entwickelten Anforderungen der Ordnungsmäßigkeit dokumentiert, um das Haftungsrisiko der einstellenden Ärzte für ihren Verantwortungsbereich der Dokumentation möglichst zu reduzieren. In den Vertrag ist die Pflicht zu integrieren, dass der Provider verschlüsselte Daten verwaltet. Damit ist gesichert, dass der Provider die Gesundheitsdaten nicht einsehen kann und wird die ärztliche Schweigepflicht gewahrt. Die zentrale Stelle ist unter dieser Bedingung funktionslos. Einstellender und abrufender Arzt können auf Grund eines solchen Auftragsdatenverhältnisses direkt auf die Daten bei dem Provider zugreifen, wenn sie dazu durch den Behandlungsvertrag berechtigt sind.

8.5 Die Datentreuhänderlösung

- Datentreuhänderschaft und Pseudonymisierung

Als Alternative zur Verschlüsselungstechnik kommt für die Speicherung von Gesundheitsdaten die Pseudonymisierung durch Datentreuhänderschaft in Frage. Die Datentreuhänderschaft, auf die Situation der eEPA angewandt, bedeutet, dass der Datentreuhänder Patientendaten mit den dazugehörigen Inhalten von dem einstellenden Arzt erhält und pseudonymisiert, hierüber eine elektronische Patientenliste führt und die pseudonymisierten Inhalte an die datenspeichernde Stelle übermittelt.

- Datenschutz

Wird durch die informationelle Gewaltenteilung der Grundrechtseingriff vermieden, so ist eine Einwilligung nicht erforderlich. Dies bedingt, dass kein Rechtsverlust besteht, also das Auskunftsrecht und die übrigen Betroffenenrechte realisierbar sind. Dem Betroffenen wird eine Stelle benannt, an die er sich wenden kann, um seinen Auskunftsanspruch und die anderen Betroffenenrechte geltend zu machen. Hierfür bietet sich die Datentreuhänderstelle

an.⁹² Die Auskunft umfasst nach dem Vorbild der automatisierten Entscheidung (§ 6a Abs. 3 BDSG) auch allgemeine Systeminformationen.

- **Beschlagnahmeschutz**

Der Beschlagnahmeschutz besteht auch, wenn durch informationelle Gewaltenteilung der Datenschutz für die Patientendaten realisiert wird, indem die datenspeichernde Stelle die von einem Datentreuhänder pseudonymisierten Dokumente erhält.⁹³ Wenn die Datentreuhänderschaft der eEPA in dieser Form organisiert wird, dann ist auch Beschlagnahmeschutz gegeben.

8.6 Haftungsrisiken des einstellenden und des abrufenden Arztes

Durch Nutzungsbedingungen für eEPA sollte für den einstellenden Arzt die Möglichkeit der „Freizeichnung“ bestimmt werden, mit der er auf die Einstellung der Dokumente entsprechend dem Zweck des Behandlungsvertrages und auf die Grenzen der Freizeichnung für vorsätzliches und grob fahrlässiges Verschulden hingewiesen wird. Für den abrufenden Arzt sollte klargestellt werden, dass er zum Abruf und zur Verwertung der Dokumente entsprechend dem Zweck des Behandlungsvertrages verpflichtet ist.

8.7 Die elektronische Gesundheitskarte in der gesetzlichen Krankenversicherung

Nach den Regeln des § 291a SGB V sind elektronische Gesundheitskarte und elektronische Patientenakte Bestandteile eines Systems, das schlagwortartig als Telemedizin bezeichnet wird. In diesem System hat die elektronische Gesundheitskarte die elektronische Patientenakte zu unterstützen. Grundlage für dieses System ist das Einverständnis des Versicherten mit dem Zugriff eines Vertreters der Heilberufe auf die elektronische Patientenakte. Danach

- ist die Einwilligung des Versicherten für die erstmalige Verwendung der elektronischen Gesundheitskarte notwendig, um Daten des Versicherten zu erheben, zu verarbeiten und zu nutzen,

⁹² Weichert, Datenschutz-Auskunftserteilung in verteilten Systemen, <http://www.datenschutzzentrum.de/vortraege/061006>

⁹³ Zu diesem Ergebnis kommt auch Dierks in seinem bisher unveröffentlichten Gutachten für die „Telematikplattform für medizinische Forschungsnetze e.V.“ wie unter <http://www.tmf-ev.de> mitgeteilt.

- ist für den auf die elektronische Patientenakte zugreifenden Arzt das Einverständnis und die Autorisierung des Versicherten und der elektronische Heilberufsausweis notwendig,
- sind auf Verlangen des Versicherten die Daten zu löschen.

Als Ergebnis bedeutet dies für die eEPA, dass § 291a SGB V die eEPA rechtlich nicht in Frage stellt und die eEPA damit rechtlich zulässig ist.

Abkürzungen

- CR Computer und Recht, Otto Schmidt Verlag, Köln.
 DuD Zeitschrift für Datenschutz und Datensicherheit, Vieweg Verlag, Wiesbaden.
 FAZ Frankfurter Allgemeine Zeitung.
 K & R Kommunikation und Recht, Verlag Recht und Wirtschaft, Frankfurt am Main.
 MMR MultiMedia und Recht, Beck-Verlag, München.
 NJW Neue Juristische Wochenschrift, Beck-Verlag, München.

Literatur

- Armgardt/Spalka*, Der Anscheinsbeweis gemäß § 371a Abs.1 S. 2 ZPO vor dem Hintergrund der bestehenden Sicherheitslücken bei digitalen Signaturen, K&R 2007, 26.
 Brockhaus Fachlexikon Computer, Mannheim 2003.
Geis, in *Spindler/Schmitz/Geis*, Kommentar zum TDG, TDDSG, SigG, München 2004.
Gola/Schomerus, Kommentar zum BDSG, 9. Aufl., München 2007.
Hornung, die digitale Identität, Baden-Baden, 2005.
Laufs, Arztrecht, 4. Aufl., München 1988.
Laufs (Hrsg.), Handbuch des Arztrechts, 3. Aufl., München 2002.
Mehrings, in *Hoeren/Sieber*, Handbuch Multimediarecht, München.
Meyer-Goßner, Strafprozessordnung, 47. Aufl., München 2004.
 Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2a (Hrsg. *Krüger*), 4. Aufl., 2003.
 Münchener Kommentar zum HGB, Band 4 §§ 238-342a (Hrsg. *Karsten Schmidt*) München 2001.
Nestor: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, herausgegeben von der nestor-Arbeitsgruppe Vertrauenswürdige Archive-Zertifizierung, Frankfurt am Main 2006.
Rossnagel., Das neue Recht elektronischer Signaturen, NJW 2001, 1817.
ders., Rechtliche Unterschiede von Signaturverfahren, MMR 2002, 215.
ders., Die fortgeschrittene elektronische Signatur, MMR 2003, 164.
ders., Elektronische Signaturen mit der Bankkarte?, NJW 2005, 385.
ders. (Hrsg.), Handbuch des Datenschutzrechts, München 2003.
Rossnagel/Fischer-Dieskau, Elektronische Dokumente als Beweismittel, NJW 2006, 806.

Rossnagel/Fischer-Dieskau/Jandt, Handlungsleitfaden Zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, herausgegeben vom Bundesministerium für Wirtschaft und Technologie, Dokumentation Nr. 564, Berlin 2007.

Rossnagel/Fischer-Dieskau/Jandt/Knopp, Langfristige Aufbewahrung elektronischer Dokumente – Anforderungen und Trends, Baden-Baden 2007.

Rossnagel/Fischer-Dieskau/Wilke, Transformation von Dokumenten, CR 2005, 903.

Rossnagel/Schmücker, Beweiskräftige elektronische Archivierung, Heidelberg 2002.

Rossnagel/Wilke, Die rechtliche Bedeutung gescannter Dokumente, NJW 2006, 2145.

Schäfer, in: *Löwe-Rosenberg*, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 25. Aufl. 2004.

Semler/Ripkens-Reinhard, Archivierung von klinischen Forschungsunterlagen, in: *Jäckel* (Hrsg.) Telemedizinführer Deutschland, Bad Neuheim, Ausgabe 2006, Seite 353-356.

Simitis (Hrsg.) Kommentar zum BDSG, 6. Aufl., Baden-Baden 2006.

VOI Dokumenten-Management, Bonn 2005.

Walz, in: *Heymann*, HGB Kommentar, 2. Aufl., Berlin 1999.

Wiedemann, in: *Ebenroth/Boujong/Joost*, HGB Kommentar, München 2001.

Zöllner, Kommentar zur ZPO, 26. Aufl., Köln 2007.

Hamburg, den 28. März 2008

Dr. Ivo Geis

Rechtanwalt