Rechtliche Aspekte der elektronischen Archivierung medizinischer Dokumente

Ivo Geis, Rechtsanwalt

Einleitung

Krankenhäuser und Kliniken sind Teil der elektronischen Gesellschaft: Um die Pflicht zur Archivierung medizinischer Dokumente zu erfüllen, werden Papierdokumente gescannt, originäre elektronische Dokumente generiert und entsprechend der medizinischen Dokumentationspflicht archiviert (Kapitel 1). An die Szenarien des Scannens von Papierdokumenten und der Archivierung originär elektronischer Dokumente werden unterschiedliche rechtliche Anforderungen gestellt. Das Scannen von Papierdokumenten ist von der Sicherheit des Scanvorgangs (Kapitel 2) und die Archivierung originärer elektronischer Dokumente von der Archivierung in elektronischer Form geprägt (Kapitel 3). Ein für die medizinische Dokumentation typischer Problemfall ist die Langzeitarchivierung, die durch die 30-jährige Verjährungsfrist wegen Schadensersatzansprüchen aus ärztlichen Kunstfehlern besteht und über diesen Zeitraum die elektronisch archivierten Dokumente integer und lesbar erhalten muss (Kapitel 4).

1 Die Pflicht zur Archivierung medizinischer Dokumente

Im Gesundheitswesen wird die ärztliche Dokumentationspflicht als Nebenpflicht aus dem Behandlungsvertrag abgeleitet und mit dem Persönlichkeitsrecht des Patienten begründet. Diese Dokumentationspflicht besteht auch nach der berufsständisch internen Regelung des

§ 10 Abs. 1 und Abs. 3 Musterberufsordnung für Ärzte (MBO).[1] Anforderungen an die Archivierung können aus den Aufbewahrungsvorschriften des HGB und der AO abgeleitet werden. Diese lassen sich auf den Nenner bringen, dass die elektronische Archivierung sicherstellen muss, dass die Daten während der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können (§ 257 Abs. 3 Satz 1 Nr. 2 HGB). Dies ist ein allgemeingültiger Grundsatz der Archivierung, der unabhängig von Handelsrecht und Steuerrecht auch für medizinische Dokumente gilt: die Integrität der archivierten Dokumente und deren Wiederauffindbarkeit.[2] Deshalb sind die handels- und steuerrechtlichen Anforderungen an die elektronische Archivierung in die Röntgen-Verordnung übernommen worden. Nach § 28 Abs. 4 RöV ist für elektronisch archivierte Röntgenbilder sicherzustellen, dass sie während der Aufbewahrungsfrist verfügbar sind, lesbar gemacht werden und keine Informationsänderungen oder -verluste eintreten können. Damit sind die Anforderungen an die Archivierung von Papierdokumenten durch Scannen und die Archivierung origninärer elektronischer Dokumente deutlich gemacht: die Integität und die Wiederauffindbarkeit des Dokuments.

2 Vom Papierdokument zum elektronischen Dokument

Das Scannen des Papierdokuments nach den Anforderungen der ordnungsmäßigen Archivierung (Kapitel 2.1) und zusätzlich mit qualifizierter elektronischer Signatur (Kapitel 2.2) sichert die Beweisqualität gescannter Dokumente (Kapitel 2.3). Aus dieser Beweisqualität ergibt sich das Recht zur Vernichtung des gescannten Papieroriginals (Kapitel 2.4).

2.1 Scannen nach den Anforderungen der Ordnungsmäßigkeit

Der Archivierungsvorgang beginnt mit dem Scannen der Papierdokumente und setzt sich in die Phase der Aufbewahrung fort. Die Anforderungen an das Scannen sind von dem Bundesfinanzministerium mit den Grundsätzen ordnungsmäßiger DV-gestützter Buchführung (GoBS) konkretisiert.[3] Hiernach ist für den Scannvorgang entscheidend, dass die Informationen des Papieroriginals in die elektronische Form übernommen werden. Dies soll nach den GoBS durch eine Organisationsanweisung sichergestellt werden, in der geregelt ist, wer scannen darf, zu welchem Zeitpunkt gescannt wird, ob eine bildliche oder inhaltliche Übereinstimmung mit dem Original erforderlich ist, wie die Qualitätskontrolle auf Vollständigkeit und wie die Protokollierung von Fehlern zu erfolgen hat.[4] Im Ergebnis muss durch die Transformation von Papierdokumenten in elektronische Dokumente sichergestellt sein, dass das Zieldokument mit dem Ausgangsdokument übereinstimmt und von wem die Übereinstimmung kontrolliert worden ist. Problematisch ist die Automation der Ergebniskontrolle von Ausgangsdokument und Zieldokument wegen möglicher technischer Risiken und Fehlinterpretationen.[5] Ein Ausschluss dieser Risiken mit letzter Sicherheit ist nicht möglich. Deshalb sollte der Transformationsprozess des Scannens durch geregelte Stichprobenkontrollen unterstützt werden.

2.2 Scannen mit qualifizierter elektronischer Signatur

Die Integration der qualifizierten elektronischen Signatur in den Scanvorgang medizinischer Dokumente findet ihre rechtliche Grundlage in dem Signaturgesetz.[6] Die qualifizierte elektronische Signatur muss nach § 2 Nr. 2 Signaturgesetz (SigG) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein 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

Autor: Ivo Geis
Titel: Rechtliche Aspekte der elektronischen Archivierung medizinischer Dokumente
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2009
Seite: 32-36

oder ein biometrisches Merkmal des Berechtigten aktiviert werden kann, § 17 Abs. 1 SigG. Diese qualifizierten elektronischen Signaturen können nach § 2 Nr. 3 SigG nur durch qualifizierte Zertifizierungsdienste vergeben werden. Um erstmals ein Signaturschlüssel-Zertifikat zu erhalten, muss der Antragsteller sich bei einer Annahmestelle eines qualifizierten Zertifizierungsdienstes mit einem gültigen Personalausweis oder Reisepass ausweisen und einen schriftlichen Antrag auf ein Zertifikat stellen, § 5 SigG.[7] Elektronisch signierte Dokumente sind unter dem Aspekt der langfristigen Aufbewahrung ein Problemfall. 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 durch Zertifizierungsdienste nachweisen. Dieses Risiko kann durch Signaturen akkreditierter Zertifizierungsdienste mimimiert werden, da diese Zertifikate mindestens 30 Jahre nach Ablauf des Gültigkeitsjahres nachprüfbar aufzubewahren sind.[8] Der Einsatz von qualifizierten elektronischen Signaturen zur Qualitätssicherung des Scannens im Gesundheitswesen ist nach den Vorgaben des Sozialgesetzbuches und der Verwaltungsvorschrift zur Sozialversicherungsrechnungsverordnung (SRVwV) vorgesehen. § 41 SRVwV regelt, dass Unterlagen, die eine qualifizierte elektronische Signatur tragen, akzeptiert werden müssen. Auf Grund der Komplexität der Abrechnung im Gesundheitswesen gelten diese Vorschriften für eine Vielzahl von Organisationen: die Träger der gesetzlichen Kranken-, Unfall-, Renten- und Pflegeversicherungen, Medizinische Dienste der Krankenversicherungen, Kassenärztliche und Kassenzahnärztliche Vereinigungen, BfA, LVAen, Krankenkassen und private Krankenversicherer.[9] Dieser Sicherheitsgedanke wurde von dem Nestor-Kriterienkatalog, den Transidoc-Grundsätzen und dem Projekt ArchiSig übernommen. 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 3 der Transidoc-Grundsätze sollte qualifizierte elektronische Signaturen mit Anbieterakkreditierung nach dem Signaturgesetz eingesetzt werden, falls ein hoher Beweiswert langfristig erforderlich ist. Das Forschungsprojekt „ArchiSig-Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ empfiehlt mit der Veröffentlichung „Beweiskräftige elektronische Archivierung“ die qualifizierte elektronische Signatur in den Scannvorgang medizinischer Dokumente zu integrieren.[10]

2.3 Die Beweisqualität gescannter Dokumente

Für die Beweisqualität elektronisch archivierter Dokumente im Rahmen der freien Beweiswürdigung spricht die Aufbewahrung nach den Grundsätzen der Ordnungsmäßigkeit. Mit der Aufbewahrung entsprechend diesen Grundsätzen wird die elektronische Dokumentation gegen Änderungen geschützt[11] und sind damit Indizien für die Beweissicherheit gegeben.[12] Die Integration der qualifizierten elektronischen Signatur in den Scanvorgang[13] ist nicht erforderlich, denn die qualifizierte elektronische Signatur wird nicht von dem Aussteller des Dokuments, sondern von der Scanstelle generiert. Damit wird lediglich erklärt, dass das Dokument von einer bestimmten Person eingescannt worden ist, nicht aber, dass das Dokument von einer bestimmten Person ausgestellt worden ist. Urkundenqualität nach § 371a ZPO entsteht durch die in den Scanvorgang integrierte qualifizierte elektronische Signatur folglich nicht. Die Beweisfunktion der qualifizierten elektronischen Signatur als Bestandteil des Scannens ist auf ein Indiz für die Integrität des Dokuments im Rahmen der freien Beweiswürdigung des Gerichts beschränkt. Die Aufbewahrung des Papieroriginals[14] ist nicht erforderlich, da durch Scannen Integrität und damit Authentizität des elektronischen Dokuments erreicht wird. Damit kann auch aus beweisrechtlichen Aspekten das Papierdokument vernichtet werden.

2.4 Das Recht zur Vernichtung des Originals

Das Scannen nach den Anforderungen der Ordnungsmäßigkeit mit oder ohne qualifizierte elektronische Signatur sichert die Integrität und Wiederauffindbarkeit des gescannten Dokuments. Die hierdurch begründete Beweisqualität des elektronischen Dokuments

ermöglicht es, auf Papierdokumente, die gescannt worden sind, zu verzichten und sie zu vernichten. [15] Eine rechtliche Pflicht zur Aufbewahrung gescannter medizinischer Dokumente besteht nicht und eine Erlaubnis zur Vernichtung der gescannten Papierdokumente ist nicht erforderlich.

3 Die Archivierung des originär elektronischen Dokuments

Die Telematik im Gesundheitswesen produziert eine ständig wachsende Zahl medizinischer Dokumente, wie den elektronischen Arztbrief und den elektronischen OP-Bericht. Zur Archivierung originärer elektronischer Dokumente geben die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) einen Hinweis. Der zentrale Gedanke der GDPdU ist, originäre elektronische Dokumente elektronisch zu archivieren, um Datenverlust durch Medienbruch zu vermeiden (Kapitel 3.1) und die Beweisqualität zu sichern (Kapitel 3.2).

3.1 Elektronische Archivierung zur Vermeidung eines Datenverlusts

Im Focus der „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) steht das originäre elektronische Dokument. 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.[16] Die Anweisungen der GDPdU haben einen allgemeingültigen Charakter, der auch auf medizinische Dokumente anwendbar ist: Um Datenverlust durch Medienbruch zu vermeiden, sind originär elektronische Dokumente des Gesundheitswesens elektronisch zu archivieren. Der allgemeingültige Rechtsgedanke der GDPdU, dass originäre elektronische Dokumente zur Vermeidung eines Medienbruchs und der damit verbundenen Gefahr des Datenverlusts elektronisch zu archivieren sind, ist auf die Archivierung medizinischer Dokumente anzuwenden. Damit entspricht die verbreitete Praxis, elektronische Dokumente auszudrucken oder nach dem Ausdruck einzuscannen nicht den Anforderungen an die ordnungsmäßige Archivierung.

3.2 Beweissicherheit des originären elektronischen Dokuments

Durch die Archivierung originärer elektronischer Dokumente nach den Anforderungen der Ordungsmäßigkeit werden Indizien für die Integrität und damit die Beweissicherheit der elektronisch archivierten Dokumente begründet. Um die der Urkunde nach § 371a ZPO gleichgestellte Beweisqualität zu gewinnen, ist der Aufwand der qualifizierten elektronischen Signatur notwendig. Damit ist der Aufwand der qualifizierten elektronischen Signatur ein Bestandteil der unternehmerischen Risikoanalyse. Eine rechtliche Notwendigkeit besteht hierfür nicht.

4 Die Langzeitarchivierung – ein Problemfall der medizinischen Dokumentation

Die Langzeitarchivierung medizinscher Dokumente ist eine technisch-organisatorische Herausforderung. Sie stellt Anforderungen auf der Ebene der Indexierung, um die Dokumente wiederzufinden (Kapitel 4.1), und verlangt eine Kombination von Sicherheitsfaktoren, um die Integrität der Dokumente sicherzustellen durch Speichermedien (Kapitel 4.2) und Speicherformate (Kapitel 4.3)

4.1 Langfristige Wiedergabe durch Indexierung

Die Wiedergabe von aufbewahrungspflichtigen Informationen in einem angemessenen Zeitraum ist eine Anforderung der ordnungsmäßigen Archivierung. die in § 257 Abs. 3 HGB allgemeingültig gesetzlich definiert ist. Hierzu muss das Dokument mit einem Index versehen sein, unter dem es aufgefunden werden kann.[17] 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 in ausreichendem Maße Metadaten:

- für eine formale und inhaltliche Beschreibung und Identifizierung der digitalen Objekte,
- zur strukturellen und technischen Beschreibung der digitalen Objekte,
- zur Beschreibung von Nutzungsrechten und -bedingungen

erheben. [18]

4.2 Archivierungstaugliche 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 jeweilige Speichermedium gesondert ausgeprägt sein können.[19] Nach dem „Nestor -Kriterienkatalog vertrauenswürdige digitale Langzeitarchive“ legt das Archivmanagement die erforderliche Qualität der Speichermedien fest.[20] Als Sicherung wird die persistente Speicherung auf geeigneten Medien wie Bändern, Platten, CDs, DVDs empfohlen.[21] 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. Das Kriterium der Sicherheit erfüllen die Varianten der WORM-Systeme mit der WORM, der wiederbeschreibbaren optischen Platte, der CD-R und der DVD-R. Wiederbeschreibbare optische Platte, CD-R und DVD-R bieten deutlich geringere Zugriffszeiten als die WORM. Die DVD-R gilt als aktueller Speicherstandard und damit als bevorzugtes Archivmedium.[22] Neben den WORM-Varianten sprechen für die Sicherheit RAID (Redundant Array of Independent Disks) -Systeme und NAS (Network Attached Storage) -Funktionen. RAID-Systeme verteilen das Risiko auf ein System von mehreren Magnetplatten. Ein NAS-System, das mit WORM-Funktionen ausgestattet ist, verhindert wirksam das Überschreiben.

4.3 Archivierungstaugliche Speicherformate

Die Langfristarchivierung verlangt archivierungstaugliche Formate. Als archivierungs-taugliches Textformat gilt PDF (4.3.1). Der Standard für Bildformate im Gesundheitswesen sind DICOM und HL7 (4.3.2).

4.3.1 Konvertierung vom Word-Dokument in das PDF-Dokument

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. Deshalb wird es als notwendig angesehen, das Format für die Langzeitarchivierung in das PDF (Portable Document Format) zu konvertieren. [23] Für PDF spricht, dass es 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.[24] Für PDF spricht auch, dass das Format verschiedene Sicherheitsmechanismen unterstützt. 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.[25] Die negative Bewertung von Word als Format für die Langfristarchivierung könnte sich ändern. Nach den Auflagen der EU-Kommission vom März 2004 und den bestätigenden Entscheidungen des Europäischen Gerichtshofs garantiert Microsoft seinen Wettbewerbern in Zukunft die Schnittstelleninformationen zugänglich und nutzbar zu machen, die für die Entwicklung von Windows-basierter Software nötig sind. [26] Durch diese Transparenz könnte Microsoft Word mit Blick auf die langfristige Aufbewahrung in positivem Sinne neu bewertet werden.

4.3.2 Bildformate im medizinischen Bereich

Als Kommunikations- und Dokumentationsstandard im Gesundheitswesen gelten die Formate DICOM und HL7. Der DICOM-Standard ist von nahezu allen Anbietern von Picture Archive and Communication Systems (PACS) übernommen worden und ist damit das Standardformat für Röntgenbilder. Präsentationswerkzeuge stehen von verschiedenen Herstellern 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 Datenfelder, um die Vertraulichkeit von Patientenidentifikationsdaten zu sichern, und durch ein proprietäres Signaturdatenformat.[27] HL7 ist ein internationaler Kommunikationsstandard für das Gesundheitswesen. In Deutschland ist die HL7-Version 2.4 unter der DIN-Norm 58965 publiziert. 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.[28]

5 Ergebnis

Die Pflicht zur Dokumentation medizinischer Dokumente wird durch elektronische Archivierung erfüllt (Kapitel 1). Papierdokumente können nach dem Scannen vernichtet werden (Kapitel 2). Originär elektronische Dokumente müssen elektronisch archiviert werden, um das Risiko des Datenverlustes durch Medienbruch zu vermeiden (Kapitel 3). Die eigentliche Herausforderung der Archivierung medizinischer Dokumente liegt in der Dauer der Archivierung, bedingt durch die Verjährungsfrist für Arzthaftungsansprüche von 30 Jahren:

Bei Innovationszyklen, die die elektronischen Archivsysteme im Abstand von wenigen Jahren erfassen und den damit verbundenen notwendigen Migrationen müssen die Dokumente integer und auffindbar sein (Kapitel 4).

Abkürzungen

CR	Computer und Recht, Otto Schmidt Verlag, Köln
DuD	Zeitschrift für Datenschutz und Datensicherheit
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

Ebenroth/Boujong/Joost, HGB Kommentar, München 2001.

Geis, in: Spindler/Schmitz/Geis, Kommentar zum TDG, TDDSG, SigG, München 2004.

Hoeren/Sieber, Handbuch Multimediarecht, München.

Münchener Kommentar zum HGB, Band 4 § § 238-342a, München 2001.

Nestor: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, herausgegeben von der Nestor-Arbeitsgruppe Vertrauenswürdige Archive-Zertifizierung, Frankfurt am Main 2006.

Roßnagel, Das neue Signaturgesetz, MMR 2001, 201.

ders., Das neue Recht elektronischer Signaturen, NJW 2001, 1817.

Roßnagel/Fischer-Dieskau/Jandt, Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, herausgegeben vom Bundsministerium 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/Fischer-Dieskau/Jandt/Wilke, Scannen von Papierdokumenten, Baden-Baden 2008.

Roßnagel/Schmücker, Beweiskräftige elektronische Archivierung, Heidelberg 2002.

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

Schmücker/Pordesch, Beweiskräftige und sicher Erzeugung und Langzeitarchivierung signierter Dokumente als Basis für die Kommunikation in medizinischen Versorgungsregionen.

Semler/Ripkens-Reinhard, Archivierung von klinischen Forschungsunterlagen, in: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2006, Seite 353-356.
VOI Dokumenten-Management, Bonn 2005.

Fußnoten

1 Zur medizinischen Dokumentationspflicht siehe *Roßnagel/Schmücker,* Beweiskräftige elektronische Archivierung, S. 27 unter Ziffer 3.4.5.2.
2 Hierauf weisen auch hin *Semler/Ripkens-Reinhard,* Telemedizinführer Deutschland 2006, 353 f.
3 BStBl. I 1995, S. 738.
4 So GoBS, VIII b) Nr. 1, in: BStBl. I 1995, S. 738, 739.
5 *Roßnagel/Fischer-Dieskau/Wilke,* CR 2005, 903, 907.
6 Grundsätzlich zu diesem Verfahren *Schmücker/Pordesch,* Telemedizinführer Deutschland,2002.
7 Zu qualifizierten elektronischen Signaturen: *Geis* in *Spindler,/Schmitz/Geis,* Kommentar zum TDG, TDDSG, SigG, Einführung zum SigG, Rz. 12-21; *Roßnagel,* Das neue Signaturgesetz-Grundlage des elektronischen Rechtsverkehrs, MMR 2001, 201; *derselbe,* Das neue Recht elektronischer Signaturen, NJW 2001, 1817.
8 Zur Neusignierung siehe *Rossnagel/Fischer-Dieskau/Jandt,* Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, S. 22 f.
9 VOI Dokumenten-Management, Ziffer 5.5.5.8, S. 344 f.
10 *Rossnagel/Schmücker,* Beweiskräftige elektronische Archivierung, vor allem Ziffer 3.5.
11 *Ballwieser,* in: Münch Komm HGB § 257 Rdnr. 16; *Walz,* in: Heymann, HGB, § 257 Rdnr. 6.
12 *Wiedemann,* in: Ebenroth/Boujong/Joost, HGB, § 257 Rdnr. 1.
13 Zur Integration der qualifizierten elektronischen Signatur in den Scanvorgang: *Roßnagel/Schmücker,* Beweiskräftige elektronische Archivierung, Ziffer 10.2.
14 Dies wird für notwendig gehalten von *Roßnagel/Fischer-Dieskau/Jandt/Wilke,* Scannen von Papierdokumenten, Baden-Baden 2007.
15 GoBS VIII. b) vorletzter Absatz, in: BStBl. I 1995, S. 738, 740.
16 GDPdU III. 1., in: BStBl. I 2001, S. 415.
17 GoBS VIII b) 1. und VIII, 3., in: BStBl. I 1995, S. 738, 740.
18 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.
19 GoBS VIII.b), in: BStBl. I 1995, S. 738, 739.
20 Nestor-Kriterienkatalog, Ziffer 6.2, S. 16.
21 Nestor-Kriterienkatalog, Ziffer 10.3, S. 21.
22 VOI Dokumenten-Management, Ziffer 5.2.8, S. 280-282.
23 VOI-Dokumenten-Management, Ziffer 5.1.7, S. 238-242.
24 Brockhaus Fachlexikon Computer, Stichwort „PDF".
25 Zum PDF-Format siehe: *Roßnagel/Schmücker,* Beweiskräftige elektronische Archivierung, Ziffer 7.3.1, S. 67-69.
26 Siehe zu dem Verfahren gegen Microsoft: FAZ vom 23.10.07, S. 15 „Microsoft beugt sich der EU-Kommission".
27 Zum DICOM-Standard: *Roßnagel/Schmücker,* Beweiskräftige elektronische Archivierung, Ziffer 7.3.4, S. 72.
28 *Roßnagel/Schmücker,* Beweiskräftige elektronische Archivierung, Ziffer 7.3.4, S. 72.

Kontakt
Dr. Ivo Geis
Rechtsanwalt
Glockengiesserwall 26
D-20095 Hamburg
Tel.: +49 (0) 40 / 30 10 41 26
Fax: +49 (0) 40 / 30 10 42 99
geis@ivo-geis.de
www.ivo-geis.de