Schlierseer Memorandum zum beweissicheren Scannen

Version 1.1, Stand: Februar 2008

Verfasser:

Dipl.-Inform. Med. Heino Kuhlemann[1,2,3], eHealthOpen Ltd., Schliersee

Prof. Dr. Paul Schmücker[1,2], Hochschule Mannheim

Dr. Carl Dujat[1,2], promedtheus AG, Erkelenz

Diplom-Archivar Volkmar Eder[1], Universitätsklinikum Tübingen

Dr. Christoph Seidel[1], Städtisches Klinikum Braunschweig gGmbH

[1] **Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (gmds), Arbeitsgruppe „Archivierung von Krankenunterlagen“**
Sprecher: Prof. Dr. Paul Schmücker

[2] **Berufsverband Medizinischer Informatiker e.V. (BVMI)**
Sprecher: Dr. Carl Dujat

[3] **AGPAH Arbeitsgruppe parlamentarischer Abend HealthValue**
Sprecher: Dipl.-Inform. Med. Heino Kuhlemann

Beschlussfassung der Präsidien der beteiligten Verbände

Das Präsidium der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e. V. hat dem Schlierseer Memorandum am 14. März 2008 zugestimmt und eine gesetzgeberische Maßnahme als erforderlich erachtet. Das Präsidium des Berufsverbandes Medizinischer Informatiker (BVMI) e. V. hat bereits am 20. Februar 2008 einen analogen Beschluss gefasst.

Zusammenfassung

Gescannte Dokumente werden bisher im Rahmen juristischer Angelegenheiten in der Regel nicht als Urkunden anerkannt. Sie obliegen lediglich dem Augenschein des Richters und stellen somit eine rechtliche und finanzielle Unsicherheit dar. Während das Signaturgesetz die Anerkennung digital erzeugter Dokumente regelt, besteht heute noch eine gesetzliche Regelungslücke für gescannte Dokumente. Zur Verbesserung dieser Situation müssen Gesetze und Verordnungen erweitert sowie technische und organisatorische Regelwerke für alle das Scannen betreffenden Prozesse entwickelt werden. Da in den nächsten Jahren nur eine gemeinsame Existenz von gescannten und digital erzeugten Dokumenten realistisch denkbar ist und somit digitale Akten gleichzeitig aus digital erzeugten und gescannten Dokumenten gebildet werden, ist eine Lösung der o. a. Rechtsfrage für die Nutzer von digitalen Archivierungssystemen und elektronischen Akten dringend notwendig. Eine rechtliche Lösung wäre zudem äußerst sinnvoll, da heutzutage

große Mengen von rechtlich relevanten Dokumenten (z.B. im Gesundheitswesen ca. 10 Prozent aller Patientenunterlagen) gescannt werden, die dargestellte Fragestellung eine Vielzahl von Einrichtungen im Rahmen der Einführung, der Erweiterung und des Betriebs von elektronischen Archivierungssystemen betrifft und viele Institutionen nicht bereit sind, digitale Archivierungssysteme vor der Klärung der rechtlichen Fragestellungen einzuführen. Die Autoren bieten eine Hilfestellung für das weitere Vorgehen beim Lösen dieser Rechtsfrage und die Praxis des rechtssicheren ersetzenden Scannens an. Dazu haben sie auch ein allgemeingültiges Regelwerk mit technischen und organisatorischen Vorgaben entwickelt. Dieses wurde auf Basis der Anforderungen des Gesundheitswesens, insbesondere von Patientenunterlagen erarbeitet.

Aktuelle Anforderungen im Gesundheitswesen

Trotz einer zunehmenden „Digitalisierung" der Dokumentation im Gesundheitswesen liegen in der Regel nach wie vor mehr als 50 Prozent der Dokumente nur auf Papier vor. Dies kann und wird durch die Einführung der Elektronischen Gesundheitskarte und des Elektronischen Heilberufsausweises nicht maßgeblich verändert werden können, da die Dokumentationsprozesse im Gesundheitswesen komplex und sehr verschiedenartig sind und darüber hinaus eine Mischwelt von papierbasierten und digital gestützten Prozessen auf absehbare Zeit bestehen bleiben wird. In der Regel ist es derzeit nicht möglich, bei einer Elektronischen Patientenakte grundsätzlich davon auszugehen, dass alle Inhalte digital erzeugt werden und in den verschiedenen Behandlungsprozessen und sonstigen Vorgängen auch in dieser Form unverändert erhalten bleiben. Eine umfassende Elektronische Patientenakte ist daher nur realisierbar, wenn sie aus gescanntem Papier und originär digital erzeugten Dokumenten besteht und auch in dieser Mischform rechtlich vollständig anerkannt ist.

Die erforderliche logische Schlussfolgerung ist, **den mit dem Digitalisieren von Papier verbundenen rechtlichen Status eines ordnungsgemäß gescannten Dokumentes zu verbessern**. Es wird prognostiziert, dass die Integration von papierbasierten und digitalen Prozessen in den nächsten 15 Jahren eine zentrale Herausforderung ist, welche derzeit **vom Gesetzgeber nicht ausreichend berücksichtigt** ist (vgl. auch [2]). Hier sehen die Verfasser, alle beteiligten Verbände und die Leistungserbringer im Gesundheitswesen einen dringenden und seit vielen Jahren überfälligen Handlungsbedarf des Gesetzgebers.

Insgesamt werden im deutschen Gesundheitswesen ca. 5,5 Mrd. Dokumente pro Jahr erzeugt, allein die Kosten für deren Archivierung betragen ca. 2,5 Mrd. € [1]. Im Gesundheitswesen sind bis zu 50 Prozent dieser Summe, d. h. ungefähr 0,5 bis 1 Mrd. € pro Jahr, als quantitatives Einsparungspotential durch Reduzierung von Sachkosten und Verbesserungen der Behandlungsprozesse nutzbar. Der wichtigere Nutzen liegt jedoch in einer höheren Qualität und einer Optimierung der medizinischen Versorgungsprozesse durch eine verbesserte Informationslogistik, also letztendlich in einer deutlich erhöhten Effizienz bei der Behandlung von Patienten.

Neben den originären Papierdokumenten bedürfen auch diejenigen digital erzeugten Dokumente einer Berücksichtigung, welche aus organisatorischen und formalen Gründen sowie im Hinblick auf eine etwaige Beweiserleichterung nach wie vor ausgedruckt, dann handschriftlich unterzeichnet und aufbewahrt werden. Papier verursacht hohe Kosten und steht zudem in den digital gestützten Arbeitsprozessen nicht zur Verfügung (vgl. Anlage 2, [1]).

Insbesondere Elektronische Fallakten (vgl. www.fallakte.de), Elektronische Gesundheitsakten und weitere freiwillige Anwendungen der Elektronischen Gesundheitskarte (eGK) sind nur dann sinnvoll einsetzbar, wenn das Problem des Umgangs mit gescannten Dokumenten dauerhaft gelöst wird.

Die Stellungnahme des Bundesministeriums für Gesundheit (BMG) zum ersetzenden

Scannen (siehe Anlage 3) greift an dieser Stelle zu kurz und berücksichtigt nicht die gängige Praxis sowie die Anforderungen bei den Leistungserbringern. Die Auffassung aus dem BMG-Schreiben „Die ärztliche Dokumentation in Papierform bedarf keiner Unterschrift, ……“ verkennt den klinischen und medizinischen Alltag, in welchem finalisierte und abgeschlossene Dokumente üblicherweise unterzeichnet werden und somit eine wesentlich höhere Beweiskraft erlangen. Dies gilt insbesondere auch für die ständig zunehmende einrichtungs- und sektorenübergreifende Kommunikation. Die darüber hinaus gehenden Ausführungen der Unzuständigkeit des BMG stellen eine Aufforderung dar, die zuständigen Ministerien und Institutionen zusammen mit Gesundheitsexperten und Juristen (z. B. Prof. Dr. Alexander Roßnagel und seine Arbeitsgruppe, Universität Kassel) anzusprechen, um das vorgelegte Problem möglichst Ressort übergreifend zu lösen.

Als weitere Partner könnten die Ärztekammern in ihrer Zuständigkeit für nachvollziehbare und wirtschaftliche ärztliche Dokumentationen sowie die Krankenhausgesellschaften als Vertreter der Krankenhäuser Unterstützung bei der Lösungsfindung leisten.

An dieser Stelle wird auch darauf hingewiesen, dass eine Empfehlung zur rechtssicheren Aufbewahrung von gescannten Dokumenten den Einrichtungen des Gesundheitswesens umfangreiche Aufwände und hohe Kosten ersparen wird. Eine derartige Empfehlung führt mit Sicherheit zu einer höheren Investitionsbereitschaft in digitale Archivierungssysteme und damit zu einer Optimierung der Behandlungsprozesse im Gesundheitswesen.

Zentrale Forderung nach gesetzgeberischem Regelungsbedarf

Für Dokumente, die im Original digital vorliegen und qualifiziert digital signiert sind, ist der gesetzliche Rahmen hinreichend [3]. **Der gleiche Status der Anerkennung** muss **für gescannte Dokumente** (sog. NCI = Non Coded Information = gescanntes Dokument) erreicht werden, wenn der Scannprozess entsprechenden Regeln der Ordnungsmäßigkeit, Nachvollziehbarkeit und Beweissicherheit genügt. Eine Echtheitsvermutung vor Gericht für vorgelegte NCI-Dokumente sollte folglich gesetzlich verbindlich geregelt werden.

Dazu ist mit den zuständigen Stellen in Ministerien und Ärztekammern sowie ggf. hinzuzuziehenden Rechtsexperten zu klären, welche Maßnahmen oder Verordnungen konkret in welchem Gesetz zu verankern sind. Dabei wäre evtl. die Musterberufsordnung für die deutschen Ärztinnen und Ärzte (MBO-Ä) und gegebenenfalls auch die Musterverordnung für die Zahnärzte und Zahnärztinnen empfehlenswert. **Aber sicher ist die bessere und allgemein nutzbare Lösung eine branchenübergreifende, allgemein rechtlich anerkannte Regelung für gescannte Dokumente.**

Mindestens muss es eine auf die Bedürfnisse des Gesundheitswesens zugeschnittene Lösung geben, aus der die Verantwortlichen im Bereich der Leistungserbringer den Umgang mit gescannten Dokumenten klar und verbindlich entnehmen können.

Dafür werden zusätzlich zu den rechtlichen Regelungen Vorgaben in Form von Regelwerken für das ersetzende Scannen von Dokumenten und die Aufbewahrung von gescannten Dokumenten benötigt [4,5]. Kernpunkte dieses Regelwerks sind die Vollzähligkeit, Vollständigkeit, Verfügbarkeit, Reproduzierbarkeit, Unveränderbarkeit, Ordnungsmäßigkeit, Revisionsfähigkeit und Beweissicherheit von gescannten Dokumenten. Ein weitgehend branchenübergreifender, allgemein gültiger Vorschlag hierfür kann der Anlage 1 entnommen werden.

Weiteres Vorgehen

Die Verfasser legen das vorliegende Schlierseer Memorandum den zuständigen Ministerien (Bundesministerium der Justiz, Bundesministerium des Innern, Bundesmini-

sterium für Wirtschaft und Technologie, Bundesministerium für Gesundheit) vor und bieten an, dieses praxisnah durch das Aufzeigen einfach nachvollziehbarer Lösungen für das rechtssichere ersetzende Scannen zu erläutern. Darüber hinaus wird das Memorandum auch den Ärztekammern und weiteren Organisationen sowie ausgewählten Bundestagsabgeordneten fraktionsübergreifend zur Verfügung gestellt.

Ist eine allgemeingültige gesetzgeberische Lösung nicht möglich, so wird empfohlen, dass die Ärztekammern gescannte Dokumente in ihren Ärzteberufsordnungen zulassen. Unabhängig hiervon sind Verfahrensregeln im Rahmen des Scannens erforderlich. Es ist auch zu prüfen, inwieweit der Bundesmantelvertrag für Ärzte (BMV-Ä) entsprechende Regelungen aufnehmen kann.

Die letzte - wenngleich am wenigsten weitreichende – Möglichkeit wäre es, wenn nur ein Regelwerk für das rechtssichere ersetzende Scannen bereitgestellt wird. Wie bereits oben erwähnt, würde diese Lösung jedoch zumindest für eine höhere Rechtssicherheit sorgen und den Betreibern von digitalen Archivierungslösungen praktische Empfehlungen für die Einführung und den Betrieb zur Verfügung stellen.

Literatur

[1] Häber, Anke; Dujat, Carl; Schmücker, Paul: Leitfaden für das rechnerunterstützte Dokumentenmanagement und die digitale Archivierung von Patientenunterlagen im Gesundheitswesen. GIT-Verlag: Darmstadt 2005.

[2] Kuhlemann, Heino: Beweissicherung bei der Archivierung digitaler Unterlagen. In: Management & Krankenhaus 05/2006, 28.

[3] Roßnagel, Alexander; Schmücker, Paul (Hrsg.): Beweiskräftige elektronische Archivierung. Bieten elektronische Signaturen Rechtssicherheit? Economica Verlag: Heidelberg, München, Landsberg, Berlin 2006.

[4] Roßnagel, Alexander; Fischer-Dieskau, Stefanie; Jandt, Silke; Wilke, Daniel: Scannen von Papierdokumenten - Anforderungen, Trends und Empfehlungen. Nomos Verlagsgesellschaft: Baden-Baden 2008.

[5] VOI Verband Organisations- und Informationssysteme e. V., TÜV Informationstechnik GmbH: PK-DML - Prüfkriterien für Dokumentenmanagementlösungen, 2. überarbeitete Auflage. VOI Verband Organisations- und Informationssysteme e. V.: Bonn 2004.

Anlagen

[1] Regelwerk für das ersetzende Scannen und die ordnungsgemäße, revisions- und beweissichere Archivierung gescannter Dokumente
[2] Schreiben an das Bundesministerium für Gesundheit vom 14. April 2006.
[3] Stellungnahme des Bundesministeriums für Gesundheit vom 06. Juli 2006.

Hinweis der Autoren

Die Version 1 wurde im Zeitraum von Herbst 2006 bis Frühjahr 2007 erarbeitet. In Version 1.1 wurde das Regelwerk von November 2007 und Februar 2008 ergänzt.

Korrespondenzpartner

Prof. Dr. Paul Schmücker
Hochschule Mannheim, Fakultät für Informatik
Institut für Medizinische Informatik
Paul-Wittsack-Straße 10, D-68163 Mannheim
Tel.: 0621/292-6206, Mobil: 0160/96772262
eMail: p.schmuecker@hs-mannheim.de

Anlage 1

Regelwerk für das ersetzende Scannen und die ordnungsgemäße, revisions- und beweissichere Aufbewahrung gescannter Dokumente

Das vorliegende **funktionale, technische und organisatorische Regelwerk** soll eine ordnungsgemäße, revisionssichere und rechtlich anerkannte Arbeit beim ersetzenden Scannen von Akten und anderen Unterlagen sowie bei der Aufbewahrung der gescannten Objekte gewährleisten. Ersetzendes Scannen bedeutet die Vernichtung der ursprünglichen Unterlagen nach Abschluss des Scannvorgangs.

Ordnungsmäßigkeit und Revisionssicherheit sind z. B. gegeben, wenn die Gestaltung der digitalen Archivsysteme an die Vorgaben der Grundsätze der ordnungsgemäßen Buchführung (GoB) und die Grundsätze ordnungsgemäßer Buchführungssysteme (GoBS) angelehnt ist. Beweissicherheit liegt vor, wenn Dokumente mindestens mit einer qualifizierten elektronischen Signatur versehen sind, diese beim Verlust der Sicherheitseignung der kryptographischen Algorithmen rechtzeitig erneuert und die zugehörigen Verifikationsdaten in verkehrsfähiger Form sicher im digitalen Archivsystem aufbewahrt werden. In diesem Fall kann mit hoher Wahrscheinlichkeit eine Tatsache bei einer Auseinandersetzung vor Gericht bewiesen werden.

Die Anforderungen an die Vollzähligkeit, Vollständigkeit, Verfügbarkeit, Reproduzierbarkeit, Unveränderbarkeit, Ordnungsmäßigkeit und Revisionssicherheit beim Scannen und die Sicherstellung einer hohen Beweissicherheit von gescannten Dokumenten können weitgehend durch die folgenden technischen und organisatorischen Maßnahmen gewährleistet werden.

Das vorliegende Regelwerk erhebt **keinen** Anspruch auf Vollständigkeit, es kann jederzeit weiter detailliert werden. Es ist aus der Sicht des Gesundheitswesens, hier insbesondere der Patientenunterlagen entwickelt worden.

Das Regelwerk beschreibt primär die spezifischen Anforderungen für das ersetzende Scannen und die Aufbewahrung gescannter Dokumente. Der zweite Punkt gilt nicht nur für gescannte Dokumente, sondern auch für das Aufbewahren von digital erzeugten und signierten Dokumenten.

A. Regeln für das ersetzende Scannen

Hierbei handelt es sich um spezifische Anforderungen des ersetzenden Scannens, nämlich an den manipulations- und fehlerfreien Prozess des Scannens und die Echtheit der ursprünglichen Dokumente.

1. Einsatzbereich des ersetzenden Scannens

Der Einsatzbereich des ersetzenden Scannens und seine Besonderheiten sind ausführlich zu dokumentieren.

2. Zeitnahes und vollständiges Scannen

Die komplette Akte ist möglichst zeitnah, vollständig und in der ursprünglichen Reihenfolge unter Beibehaltung der ursprünglichen Struktur zu scannen. Zeitnah bedeutet möglichst kurz nach dem Unterschreiben des Dokumentes. Je größer der Zeitraum zwischen Unterschrift und Scannvorgang ist, desto größer ist die Gefahr einer Behauptung vor Gericht, dass ein Dokument manipuliert worden sei. Mit Vernichtung eines Dokumentes sind in der Regel Manipulationen an dem ursprünglichen Dokument nicht mehr erkennbar.

3. Vollzähligkeit der gescannten Akten

Das letzte Dokument einer Akte sollte gesondert gekennzeichnet werden, um die

Vollständigkeit der Akte zu gewährleisten. Zusätzlich sollten die Anzahl der Dokumente und die Anzahl der Seiten einer Akte in dem digitalen Archivsystem gespeichert werden.

4. Vollständigkeit der gescannten Dokumente

Es muss sichergestellt werden, dass Dokumente ohne Informationsverlust gescannt werden.

5. Vorbereitung des Scannvorgangs

Gegebenenfalls müssen geheftete Dokumente entklammert, zusammengehörende Seiten gekennzeichnet, zerknitterte Dokumente geplättet, Falten oder umgeknickte Ecken entfernt werden. Auch sollten nicht bzw. nicht vollständig lesbare Dokumente entnommen und der vorgesetzten Stelle vorgelegt werden. Eventuell müssen auch spezielle Dokumente ausgesondert und weiterhin in ihrer Ursprungsform aufbewahrt werden.

6. Scannen auf Basis von Standards

Beim Scannen von Dokumenten sollten nur gängige Standards wie TIFF, PDF, PDF/A, JPEG oder JPEG2000 verwendet werden. Sollten Röntgenbildern gescannt werden, so bietet sich der Standard DICOM an.

7. Hinterlegen des Scannzeitpunktes

Der Zeitpunkt, zu dem ein Dokument gescannt wird, muss in den Metadaten des Dokumentes hinterlegt werden.

8. Überwachung des Scannvorgangs

Das Scannen der Dokumente muss am Bildschirm zwecks Überprüfung der Übereinstimmung und Lesbarkeit fortlaufend vom Scannpersonal überwacht werden. Auffälligkeiten wie Fälschungen oder Änderungen an Dokumenten sowie fehlende Informationen auf den Dokumenten sind an die vorgesetzte Stelle zu melden.

9. Nachträglich eintreffende Einzeldokumente

Nachträglich eintreffende Dokumente oder Dokumente aus fremden Einrichtungen sind den zugehörigen Akten eindeutig zuzuordnen.

10. Endlospapier

Am geeignetsten ist hierfür der Einsatz eines Endlosscanners. Wird das Endlospapier (z.B. EEG-Befund) in DIN A4-Größe zerschnitten, so sollten die einzelnen Seiten von 1 bis n durchnumeriert werden.

11. Farbdokumente

Farbige Dokumente müssen farbig gescannt und reproduziert werden können.

12. Durchlichtdokumente

Werden Durchlichtdokumente (z. B. Röntgenbilder) gescannt, so müssen hierfür geeignete Scanner eingesetzt werden. Auch hier gilt, die Qualität der Reproduktion muss der des Ursprungsobjekts entsprechen.

13. Indexierkonzept

Die Dokumente einer Akte müssen eindeutig dem richtigen Objekt (z. B. Patienten) zugeordnet werden und auf Basis von Metadaten (z. B. Dokumententyp, Leistungserbringer, Zeitpunkt der Leistungserbringung, Leistungsanforderer) und ihrer Merkmalsausprägungen beschrieben werden. Hierdurch muss sichergestellt werden, dass später genau das gesuchte Dokument wiedergefunden wird, die Datenschutzanforderungen beim Zugriff auf die Dokumente eingehalten werden

und gegebenenfalls die Weiterleitung von Dokumenten zielsicher gesteuert wird.

Aus rechtlichen Gründen sollten möglichst auch der Autor eines Dokumentes (z. B. der verantwortliche leistungserbringende Arzt) und der Mitarbeiter, der den Scannvorgang durchführt, dem gescannten Dokument ebenfalls als Metadaten beigefügt werden.

Zusammengehörende Seiten müssen eindeutig dem richtigen Dokument zugeordnet werden. Die Zusammengehörigkeit von Verbunddokumenten muss gekennzeichnet werden.

Es können auch automatische oder halbautomatische Indexierverfahren eingesetzt werden. Diese sind ausführlich zu dokumentieren.

14. Qualitätssicherung der gescannten Dokumente

Die Prozesse des Scannens und der Indexierung müssen qualitätsgesichert sein. In einem Stichprobenverfahren sollten ausgewählte Akten nach einem Zufallsprinzip auf Vollzähligkeit, Vollständigkeit, Reproduzierbarkeit und Übereinstimmung mit dem Original überprüft werden. Es empfiehlt sich, dass mindestens jede 200. Akte einer Prüfung unterzogen wird.

Die Qualitätssicherung sollte nicht von dem Scann- und Indexierpersonal durchgeführt werden.

15. Reproduktionen

Die Reproduzierbarkeit und Lesbarkeit der gescannten Dokumente müssen zeitnah zur Anforderung gewährleistet sein. Die Reproduktion am Bildschirm und auf dem Drucker muss bildlich und inhaltlich mit dem Original vollständig übereinstimmen (1:1-Abbildung analog den Erfahrungen mit der Mikroverfilmung). Dies betrifft auch die Farbe in Dokumenten.

16. Personenbezogene qualifizierte elektronische Signatur mit Zeitstempel

Die gescannten Dokumente sind mindestens qualifiziert elektronisch zu signieren und mindestens mit einem qualifizierten elektronischen Zeitstempel zu versehen, wenn diese die höchstmögliche Sicherheitsstufe erhalten sollen. Die elektronische Signatur erfolgt für ein oder mehrere Dokumente durch die Person, die den Scann- und Indexiervorgang oder die Qualitätssicherung der gescannten Dokumente durchführt. Bei der Signatur handelt es sich somit um personenbezogene Einzel- oder Massensignaturen. Gleichzeitig mit der Signatur sollte ein Zeitstempel eingeholt und mit den Signaturdaten gespeichert werden. Insgesamt handelt es sich folglich um eine personenbezogene Signatur mit Zeitstempel.

Bei einer 30-jährigen Aufbewahrungsfrist bietet sich eine Nutzung von qualifizierten elektronischen Signaturen akkreditierter Trustcenter an.

Mit Hilfe von Signatur und Zeitstempel kann nachgewiesen werden, welche Person zu welchem Zeitpunkt den Scannvorgang durchgeführt hat, und bei einer beweissicheren Archivierung sichergestellt werden, dass ein Dokument ab dem Scannzeitpunkt nicht manipuliert worden ist und damit seit dem Scannen unverändert archiviert wird.

Wenn man ein derartig hohes Sicherheitsniveau nicht aufbauen möchte, kann man auch nur mit einem qualifizierten elektronischen Zeitstempel arbeiten. Dieser bestätigt, dass ein Dokument zu einem bestimmten Zeitpunkt in einer bestimmten Form vorgelegen hat und gegebenenfalls seitdem nicht verändert worden ist. Aus dem Zeitstempel geht nicht hervor, wer den Scann- und Indexiervorgang durchgeführt hat.

Das Signieren der gescannten Dokumente und Einholen der Zeitstempel sollte frühestens nach dem Indexieren erfolgen, eventuell auch erst nach der Qualitätssicherung.

17. Vernichtung der ursprünglichen Dokumente
Die Vernichtung der Dokumente darf erst erfolgen, wenn für diese das Scannen, das Indexieren und das Signieren sowie die qualitätssichernden Maßnahmen abgeschlossen sind.

18. Verfügbarkeit geeigneter technischer Komponenten für das Scannen
Zu den Scannsystemen sind detaillierte Dokumentationen erforderlich. Durch Voreinstellungen (z. B. Auflösung, Farbtiefe) und technische Sicherheitsmechanismen (z. B. Doppeleinzugskontrolle, gleichzeitiges Scannen von Vorder- und Rückseiten) muss sichergestellt werden, dass ordnungsgemäß gescannt wird.

19. Nutzung einer standardisierten Schnittstelle
Zwischen den Scann-/Indexier-, Signatur- und Archivierungsdiensten sollten möglichst standardisierte Schnittstellen eingesetzt werden (z. B. der internationale IETF-Standard RFC 4998 Evidence Record Syntax (ERS)). Diese Schnittstellen sollten detailliert und vollständig beschrieben und getestet werden.

20. Arbeitsanweisungen und Prozessbeschreibungen
Es sind einfach verständliche und vollständige Arbeitsanweisungen und Prozessbeschreibungen für das Scannen und Indexieren zu erstellen.

21. Ausreichendes Schulungsangebot
Für das Scann- und Indexierpersonal sind geeignete Schulungsmaßnahmen und Nachschulungen durchzuführen. Dafür ist ausreichendes Schulungsmaterial bereit zu stellen. Es sollte jedoch darauf geachtet werden, dass die Bedienung der Software möglichst selbsterklärend funktioniert. Unbenommen davon sind Schulungen zur Scannqualität, zur Indexierung und Qualitätssicherung erforderlich.

22. Einsatz von vertrauenswürdigem Personal
Geeignete persönliche Voraussetzungen sind beim Einsatz des Scannpersonals zu gewährleisten, insbesondere da es sich beim Scannen und Signieren um vertrauliche Tätigkeiten (z. B. in Form von Beglaubigungen) handelt. Die Tätigkeiten des Scannens und Indexierens sowie die Entscheidungs- und Prüfinstanzen sind beim internen und externen Scannen personell strikt voneinander zu trennen. Es ist eine Unabhängigkeit der Dienstleister zu gewährleisten.

23. Festlegung der Zuständigkeiten
Die Entscheidungs- und Prüfinstanzen sind für das ersetzende Scannen schriftlich festzulegen.

24. Einhaltung der Datenschutzbestimmungen beim Scannen
Das Scannpersonal ist nach dem jeweils zuständigen Datenschutzgesetz auf die Einhaltung des Datenschutzes und der Verschwiegenheit zu verpflichten. Scannmitarbeiter dürfen nicht auf digitale Archive zugreifen können.

25. Zertifizierung der lokalen Scann- und Indexierverfahren
Eine Zertifizierung der lokalen Scann- und Indexierverfahren ist erforderlich.

26. Zertifizierung des Scanndienstleisters
Eine Zertifizierung des Scanndienstleisters ist erforderlich.

B. Regeln für das Aufbewahren gescannter Dokumente

Die Regeln für das Aufbewahren sind nicht nur für gescannte Dokumente sicherzustellen, sondern auch für digital erzeugte und signierte Dokumente. Hierbei ist die Unverfälschtheit des gescannten und digital erzeugten Dokumentes zu gewährleisten.

27. Wiederauffindbarkeit

Jedes Dokument muss mit geeigneten Retrievaltechniken in angemessener Zeit wieder auffindbar sein.

28. Zugriffsberechtigungskonzept

In einem mächtigen Zugriffsberechtigungskonzept muss geregelt werden, wer wann bei welchen Prozessen auf welche Informationen zugreifen darf. Ein Korrigieren und Löschen von Dokumenten ist nur in speziellen Situationen erlaubt (siehe Löschen von Dokumenten). Prüfinstanzen wie z. B. dem Medizinischen Dienst der Krankenversicherung (MDK) muss der Zugriff auf Patientenunterlagen erlaubt werden.

Die Zugriffsberechtigungskonzepte müssen in den betreffenden Softwaremodulen abgebildet sein.

29. Löschen von Dokumenten

Das Löschen von Dokumenten muss entsprechend den Auflagen der Datenschutzgesetze während ihrer Aufbewahrungsdauer gewährleistet werden.

In einem digitalen Archivsystem dürfen Dokumente grundsätzlich nicht verändert werden. Sie dürfen nur dann bzw. müssen gelöscht werden, wenn die gesetzliche Aufbewahrungsdauer abgelaufen ist. Aus diesem Grunde sollte das Löschdatum der einzelnen Dokumente in dem digitalen Archivsystem hinterlegt werden. Da z. B. die Aufbewahrungsfrist von Patientenunterlagen durch die letzte Behandlung in einer Einrichtung bestimmt wird, muss auch das Löschdatum verlängert werden können.

Wenn eine Person eine berechtigte Korrektur seiner Unterlagen fordert, so sollte das ursprüngliche Dokument gelöscht und durch ein korrigiertes ersetzt werden.

Das Löschen sollte nur nach dem Vier-Augen-Prinzip erlaubt sein. Alle Löschvorgänge müssen dokumentiert werden.

30. Archivierung erforderlicher Verifikationsdaten in verkehrsfähiger Form

Da die Verifikationsdaten zu den Signaturen nur begrenzt von dem Zertifizierungsdiensteanbieter aufbewahrt werden (5 Jahre bei qualifizierten elektronischen Signaturen, 30 Jahre bei qualifizierten elektronischen Signaturen mit Anbieterakkreditierung), sollten diese von dort beschafft und zusammen mit der Signatur abgelegt werden. Dies empfiehlt sich insbesondere bei der Nutzung qualifizierter elektronischer Signaturen, da in diesem Falle bei einem Konkurs des Zertifizierungsdiensteanbieters die Zertifikate nicht mehr zur Verfügung stehen. Bei qualifizierten elektronischen Signaturen mit Anbieterakkreditierung stellt die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) die Verfügbarkeit der Zertifikate über 30 Jahre sicher.

31. Konsequente Überprüfung der Sicherheitseignung kryptographischer Algorithmen

Ständig ist zu überprüfen, ob die bei der Signierung verwendeten Algorithmen noch sicherheitsgeeignet sind. Diese Informationen können entsprechend der Veröffentlichungen der Bundesnetzagentur (BNetzA) dem Bundesanzeiger entnommen werden.

32. Hash- und Signaturerneuerung von elektronisch signierten Dokumenten

Da die den Signaturen zugrundeliegenden Algorithmen mit der Zeit ihre Sicherheitseignung verlieren können, müssen Hash- und Signaturerneuerungen auf Basis eines zumindest qualifizierten, weiterhin gültigen Verfahrens (Zeitstempel und Hashalgorithmen) möglich sein. Ende des Jahres 2007 wurde die Signatur nach RSA 1024 (Schlüssellänge: 1024 Bit) ungültig. Für den Hashalgorithmus SHA-1 (Schlüssellänge: 160 Bit) wird eine Sicherheit bis 2010 prognostiziert, für den SHA-256 bis 2014. Zum Erhalt der Beweissicherheit der nach RSA 1024 signierten Dokumente musste eine Neusignierung nach RSA 2048 vor Beginn des Jahres 2008 durchgeführt werden.

33. Erhöhte Sicherheit beim Einsatz von Signaturen durch Redundanz

Bei der Speicherung und Erneuerung elektronisch signierter Dokumente kann man eine erhöhte Sicherheit erreichen, indem man Signaturen und Wurzelzertifikate mit unterschiedlichen Algorithmen erzeugt. Mit Sicherheit werden nicht gleichzeitig verschiedene Signaturalgorithmen ihren Sicherheitswert verlieren.

34. Konsequente Nutzung von Standards

Es sollten nur eindeutig interpretierbare, langfristig stabile und international standardisierte Nutzdaten- und Signaturdatenformate Verwendung finden. Bei den Nutzdatenformaten empfehlen sich TIFF, PDF, PDF/A und DICOM, bei den Signaturdatenformaten CMS, PKCS #7 und XML-DSig, als Hashalgorithmen SHA-256, SHA-512, MD5 und RIPEMD-160 sowie bei den die Dokumente beschreibenden Metadaten XML.

Für die Neusignierung von Dokumenten und die Beschaffung der Verifikationsdaten sollte der ERS-Standard (ERS - Evidence Record Syntax) der Working Group „Long-Term Archiving and Notary Services (LTANS)“ der Internet Engineering Task Force (IETF) genutzt werden.

35. Migration

Migrationen des digitalen Archivguts sind nicht vermeidbar, z. B. bei einem Wechsel des Speichersystems, einem Software-Update oder einem Wechsel von Soft-/Hardware-Komponenten. Wegen der rasanten technologischen Weiterentwicklung der Speichermedien ist in der Regel mit einer Migration nach 7 bis 10 Jahren zu rechnen, insbesondere da dann die Lese- und Schreiblaufwerke nicht mehr gewartet werden und die Kosten der Wartung und Speichermedien stark reduziert werden können.

Für die Migration wird eine geeignete Migrationssoftware benötigt. Bei einer Migration darf kein Informationsverlust auftreten, auch dürfen keine Informationen hinzugefügt oder modifiziert werden. Signaturen zu Dokumenten müssen ihre Gültigkeit behalten.

Durch eine ausschließliche Nutzung von gängigen Standards wie TIFF, PDF, PDF/A, JPEG, JPEG2000 oder DICOM kann mit hoher Sicherheit eine Transformation von Dokumenten vermieden werden. Eine Migration ohne Transformation ist relativ problemlos durchzuführen, wenn Dokumente lediglich unverändert von einem Medium auf ein anderes Medium kopiert werden. Eine rechtssichere Transformation von digitalen Dokumenten kann bisher trotz des Projektes „TransiDoc - Rechtssichere Transformation signierter Dokumente“ (siehe auch www.transidoc.de) noch nicht sicher gewährleistet werden.

Eine Migration muss ordnungsgemäß dokumentiert werden und zu einem späteren Zeitpunkt nachvollziehbar sein.

36. Verfügbarkeit geeigneter technischer Komponenten für Signaturen

Geeignete technische Komponenten zur Signaturerzeugung, Neusignierung, Verifikationsdatenbeschaffung und Signaturverifikation müssen über den gesamten Lebenszyklus eines Dokumentes zur Verfügung stehen und ausreichend dokumentiert sein.

Die bei den Signaturverfahren eingesetzten Signaturerstellungseinheiten sollten durch die Bundesnetzagentur (BNetzA) zertifiziert sein, zu den Signaturanwendungskomponenten sollte eine Herstellererklärung vorliegen, in der der Hersteller gegenüber der zuständigen Aufsichts- und Kontrollinstitution erklärt, dass sein Produkt allen hierfür relevanten technischen Standards und Spezifikationen genügt.

Zusätzlich sind Server, Clients, Speichersysteme, das Netz und die Datenträger ausführlich zu dokumentieren. Die eingesetzten Systeme müssen den Grundsätzen der Ordnungsmäßigkeit, Revisionssicherheit und der IT-Sicherheit genügen.

37. Nutzung selbsterklärender Dokumente

Aufgrund zahlreich anstehender Migrationen und des erhöhten Kommunikationsbedarfs mit externen Einrichtungen (z. B. wegen der neuen integrierten medizinischen Behandlungsformen) sollten möglichst selbsterklärende Dokumente genutzt werden. Diese enthalten neben dem eigentlichen Dokument auch die Metadaten, die Signaturen und die Verifikationsdaten zu den elektronischen Signaturen.

38. Sicherer Transport von digitalen Dokumenten

Beim Transport der digitalen Dokumente, ihrer Metadaten und Signaturdaten darf weder ein Verlust noch eine Manipulation von Nachrichten möglich sein. Ein derartiger Kommunikationsprozess muss vom empfangenden System als „ordnungsgemäß erfolgt“ quittiert werden. Es muss sichergestellt werden, dass kein elektronisches Dokument auf dem Weg ins Archiv verloren geht.

39. Einrichtungsübergreifender Informationsaustausch

Ein Vorteil elektronisch signierter Dokumente ist auch, dass der Beweiswert der Dokumente bei einem einrichtungsübergreifenden Nachrichtenaustausch erhalten bleibt.

40. Dokumentenverlust

Kein Dokument darf während seiner Lebenszeit zerstört oder vernichtet werden können. Es muss sichergestellt werden, dass kein Dokument im digitalen Archiv verloren geht.

41. Dokumenten- und Datensicherung

Alle digitalen Daten- und Dokumentenbestände sind nach gängigen und anerkannten Verfahren zu sichern.

42. Protokollierung der Transaktionen im digitalen Archiv

Alle Transaktionen wie Ablegen und Löschen von Dokumenten sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Archivzustandes mit Hilfe der Daten- und Dokumentensicherung sowie der Transaktionssicherung möglich ist.

43. Systemabnahmen und ausführliche Programmdokumentationen

Es muss gewährleistet werden, dass ausführliche Programm- und Systemdokumentationen vorliegen. Release- und Systemwechsel sowie individuelle

Softwareanpassungen müssen ebenfalls ausreichend dokumentiert und getestet werden. Aussagekräftige Freigabeprozeduren sind bei der Installation und dem Releasewechsel von Software vorzusehen und geeignet zu dokumentieren. Dadurch soll die Korrektheit, Ordnungsmäßigkeit und Revisionsfähigkeit der Archivierungslösung sichergestellt werden.

Eine wichtige Hilfe im Rahmen der Freigabe stellen Systemabnahmen dar, die auf Basis von dem Pflichtenheft, von ausreichenden Testfällen und den Fehlermeldungen in der Einführungsphase durchgeführt werden. Die Systemabnahme ist ausreichend zu dokumentieren.

44. Ausreichende Dokumentation und Auswertung von Fehlermeldungen

Fehler und Unzulänglichkeiten, die beim Scannen und Indexieren oder bei dem Aufbewahren, dem Wiederauffinden und dem Präsentieren von gescannten Dokumenten auftreten, sind in einem Fehlerbuch zu dokumentieren. Dieses ist fortwährend auszuwerten. Gegebenenfalls müssen Maßnahmen zur Behebung oder Vermeidung von Fehlern und Unzulänglichkeiten eingeleitet werden.

45. Einhaltung der Datenschutzbestimmungen beim Aufbewahren

Grundsätzlich sind die gesetzlichen sowie die betrieblichen Bestimmungen hinsichtlich Datenschutz und Datensicherheit über die Lebensdauer des digitalen Archivs sicherzustellen.

46. Gewährleistung der Sicherheit für das Gesamtsystem

Ordnungsmäßigkeit, Revisionsfähigkeit, IT-Sicherheit und Beweiswerterhalt müssen für alle Komponenten des Gesamtsystems gewährleistet werden. Auch im Datenbanksystem dürfen unberechtigterweise keine Löschungen, Einfügungen und Modifikationen zu archivierten Dokumenten vorgenommen werden können.

47. Verwendung geeigneter Speichermedien

Die Verwendung von einmal beschreibbaren Speichermedien führt heutzutage nicht mehr unbedingt zu einer höheren System- und Beweissicherheit, wenn digital erzeugte und signierte Dokumente mit ausreichendem Sicherheitsniveau (d. h. qualifizierte elektronische Signaturen oder qualifizierte elektronische Signaturen mit Anbieterakkreditierung) und geeigneten Maßnahmen des Beweiswerterhaltes (z. B. Signaturerneuerung) verwandt sowie alle Transaktionen des elektronischen Archiv aufgezeichnet und Daten- und Dokumentensicherungen durchgeführt werden. Der Vorteil von nicht wiederbeschreibbaren Speichermedien (z. B. WORM, CD-ROM, DVD-ROM, UDO) ist, dass Dokumente quasi für „ewig“ an einem bestimmten Ort aufgezeichnet werden und es erkenntlich ist, wenn Dokumente auf einem nicht wiederbeschreibbaren Medium gelöscht werden. Heute ist es auch möglich und zulässig, die Einmalbeschreibbarkeit eines wiederbeschreibbaren Mediums durch zertifizierte Softwarelösungen sicherzustellen. Auch diese Plattensysteme gelten in Kombination mit der Software als revisionssicher und können Verwendung finden.

48. Durchführung einer Risikoanalyse

Vor der Inbetriebnahme eines digitalen Archivs sollte eine Gefährdungsanalyse durchgeführt und, aufbauend auf dieser, ein Notfallkonzept erarbeitet werden. Die Risikoanalyse sollte in regelmäßigen zeitlichen Abständen aktualisiert werden.

49. Archivordnung und Verzeichnis der Archivbestände

Jede digital archivierende Institution sollte eine Archivordnung besitzen. In dieser sind alle relevanten Prozesse zu beschreiben und die Arbeitsanweisungen und

Zuständigkeiten zu hinterlegen. Zusätzlich müssen die Archivbestände jederzeit vollständig und aktuell in einem Verzeichnis einschließlich der Aufbewahrungsfristen dokumentiert sein. Änderungen in der Archivstruktur sind zeitnah aufzuzeichnen.

50. Zertifizierbare Migrationskonzepte
Für einen Wechsel des Speichersystems, einen Software-Update oder einen Wechsel von Soft-/Hardware-Komponenten müssen zertifizierbare Migrationskonzepte entwickelt werden.

51. Zertifizierung durch akkreditierte Institutionen
Die Scannverfahren, Scanndienstleister und Archivdienste sind möglichst nur von solchen Institutionen zu zertifizieren, die entsprechend akkreditiert sind.

52. Anforderungskataloge für die Zertifizierungen
Für die o. a. Zertifizierungen müssen vollständige Anforderungskataloge vorliegen und den interessierten und betroffenen Personen und Institutionen öffentlich zugänglich sein.

53. Grundsätzliches zu Zertifizierungen
Zertifizierungen können eine hohe Sicherheit bieten; Verantwortung und Restrisiko verbleiben jedoch beim Anwender.

Ziel der Vorlage des Regelwerks für gescannte Dokumente ist es, dass diese bei Einhaltung der Regeln - falls es erforderlich ist, sogar durch Hinzuziehung eines Gutachters - vor Gericht akzeptiert werden. Arbeitet man alleinig mit dem Regelwerk, so gilt nach wie vor die freie Beweiswürdigung vor Gericht. Bei Beachtung des Regelwerks erhalten die Dokumente mit Sicherheit einen wesentlich höheren rechtlichen Beweiswert. Daneben trägt das Regelwerk auch zu einer höheren betrieblichen Sicherheit bei der Nutzung von gescannten Dokumenten bei.

Anlage zum Schreiben an das Bundesministerium für Gesundheit vom 14. April 2006

Heino Kuhlemann, d.velop consulting & solutions GmbH, h.kuhlemann@consulting4solutions.de

Presse-Information

Oberhaching, 14.4.2006

Beweissicherheit bei der Archivierung digitaler Unterlagen im Gesundheitswesen – Handlungsbedarf für die Politik!

Einsparungen in Höhe von 0,5 – 1 Mrd. € pro Jahr in Deutschland durch Anpassung rechtlicher Rahmenbedingungen möglich

Papierarchive bieten unzureichende Voraussetzungen für eine effiziente Arbeitsweise in Krankenhäusern und in der intersektoralen Kommunikation: hoher Lager- und Sachkosten für teilweise Millionen von Patientenakten pro Krankenhaus, eine ineffiziente Bereitstellung einer Akte nach Anforderung, das regelmäßige Verschwinden von Unterlagen und die Tatsache, dass eine Papierakte physisch nur an einem Ort verfügbar sein kann – die Welt der Papierakten ist nur ein Beispiel für Optimierungsbedarf im Gesundheitssystem, der dringend fokussiert werden muss.

Nachfolgend sind notwendige Anpassungen gesetzlicher Rahmenbedingungen aufgezeigt, die mittelfristig einen Nutzen in Deutschland von **0,5 – 1 Mrd. € pro Jahr** an Einsparungen und eine signifikante Steigerung von Qualität und Wachstumsimpulse für die Wirtschaft bewirken.

Der Gesetzgeber muss den Weg für enorme Einsparungen und Impulse für Hochtechnologie frei machen, ohne selbst für die Finanzierung sorgen zu müssen. Auch die Einführung der elektronischen Gesundheitskarte (eGK) und des elektronischen Heilberufeausweises (eHBA) löst das nachfolgend geschilderte Problem nicht!

Im deutschen Gesundheitswesen ist Nachholbedarf im Hinblick auf die konsequente Nutzung **nachträglich digitalisierter** Unterlagen festzustellen – denn nachträglich digitalisierte Unterlagen sind auch nach Einführung der eGK und des eHBA überwiegender Teil einer lebenslangen Patientenakte oder z.B. einer Fallakte eines Patienten, deren 30-jährige Aufbewahrungspflicht in einem Krankenhaus zu erfüllen ist. Patientenakten bestehen auch in Zukunft nicht nur aus einem elektronischen Arztbrief bzw. elektronisch erzeugten und qualifiziert signierten Dokumenten oder strukturierten Einzelinformationen. Das gilt sowohl für dann noch vorhandene Altakten eines Patienten als auch für seine künftigen Akten.

In den vergangenen Jahren wurde die Diskussion um die Beweissicherheit digital archivierter Patientenunterlagen (archivierte Patientenakte = APA als langzeitstabile Form der elektronischen Patientenakte = EPA) regelmäßig öffentlich geführt. Die politisch notwendigen Konsequenzen / Handlungen sind jedoch nicht erfolgt – vgl. www.consulting4solutions.de

Es sei angemerkt, dass die heutigen Aktivitäten der Politik in Richtung **elektronische Patientenakte** (ePA) das unten beschriebene Problem nicht lösen, da es im Bundesministerium für Gesundheit (BMG) derzeit keine Definition der **archivierten Patientenakte** unter Berücksichtigung heute bewährter Verfahren gibt.

Ziel der **ordnungsmäßigen digitalen Archivierung** ist es im Idealfall, durch geeignete technische Lösungen und adäquate organisatorische Maßnahmen eine *Echtheitsvermutung* für Dokumente vor Gericht zu erzielen – d.h. der Richter vermutet die Echtheit des Dokuments, Zweifel an der Echtheit wären Aufgabe der Beweisführung der Gegenpartei. Wenn eine Echtheitsvermutung gegeben ist, so ist das digitale Dokument dem Papier gleichgestellt.

Die Echtheitsvermutung in den für Krankenhäuser und Arztpraxen gültigen rechtlichen Rahmenbedingungen gilt nach Signaturgesetz **nur für das digital erzeugte Dokument** (Coded Information = CI), das qualifiziert digital signiert ist. Hierbei ist das **digital erzeugte Dokument das Original**. eRezept und eArztbrief sind Beispiele möglicher Dokumentenarten.

Wo jedoch eine Echtheitsvermutung nicht erreicht werden kann (**Stand heute bei gescanntem Papier**), muss durch einen Nachweis der Digitalisierungs- und Speicherverfahren sowie eine Dokumentation der verwendeten Technologie die Anerkennung vor Gericht im Rahmen der „freien Beweiswürdigung" erreicht werden. Hier waren und sind Krankenhäuser und Arztpraxen verunsichert und halten daher vielfach nach wie vor an Papierarchiven fest.

Liegt also das **Original auf Papier** vor (Non Coded Information = NCI), sind auf Grund teilweise fehlender rechtlicher Regelungen hohe Anforderungen an die eingesetzte Technologie und die Verfahrensdokumentation zu stellen, um im Rahmen der freien Beweiswürdigung durch den Richter eine Anerkennung mit an Sicherheit grenzender Wahrscheinlichkeit zu erreichen.

Noch nicht hinreichend geregelt ist demnach die Fragestellung, unter welchen Voraussetzungen gescanntes und durch das Scan-Personal signiertes Papier vernichtet werden kann.

Hierzu gibt es lediglich Ausnahmeregelungen im Bereich der Sozialversicherungen unter Berufung auf §110 SGB IV. Notwendig ist jedoch eine einheitliche Regelung, die zur Echtheitsvermutung der vorgelegten **nachträglich digitalisierten Dokumente / Urkunden** vor Gericht führt, die auch für Krankenhäuser und Arztpraxen greift.

Voraussetzungen und Rahmenbedingungen sollten definiert werden: Ein einfaches und ungeprüftes Scannen ist selbstverständlich nicht hinreichend. Eine *Beglaubigung* (= Signatur beim Scannen) durch hauseigenes Personal ist nur unter bestimmten Voraussetzungen zielführend. Vorstellbar ist eine Verordnung, die eine zertifizierte Prozessbeschreibung fordert und definiert, wer den Scan-Prozess durch eine digitale Signatur beglaubigt. Erst durch die Einhaltung dieser heute noch fehlenden Regelungen sind **Gesundheitsakten / Patientenakten,** welche aus einer Mischung von gescannten und digital erzeugten Dokumenten bestehen, **rechtskonform und sinnvoll aufzubauen**. Papier könnte dann ohne Bedenken vernichtet werden.

Anlage 3

Stellungnahme des Bundesministeriums für Gesundheit vom 06. Juli 2006

Bundesministerium
für Gesundheit

Bundesministerium für Gesundheit, 53109 Bonn

d.velop consulting & solutions GmbH
Herrn Heino Kuhlemann
Bajuwarenring 12a
82041 Oberhaching

REFERAT Gruppe Telematik-Z 25
BEARBEITET VON Gerlinde Schmitt

HAUSANSCHRIFT Am Propsthof 78a, 53121 Bonn
POSTANSCHRIFT 53109 Bonn

TEL +49 (0)228 941-3152
FAX +49 (0)228 941-4997
E-MAIL gerlinde.schmitt@bmg.bund.de
INTERNET www.bmg.bund.de

Bonn, 06. Juli 2006
AZ GT-105500

Beweissicherung bei der Archivierung digitaler Unterlagen im Gesundheitswesen

Sehr geehrter Herr Kuhlemann,

vielen dank für Ihre E-Mail an Frau Ministerin Schmidt vom 28. April 2006, mit der Sie Ihre Presse-Information zum Thema "Archivierung von Patientenunterlagen" übersenden. Ich bin beauftragt worden, Ihnen zu antworten.

Sie stellen als Ziel einer digitalen Archivierung von Patientenakten die Erreichung einer Echtheitsvermutung des elektronischen Dokuments vor Gericht dar. Die Vermutung der Echtheit besagt, dass ein Dokument unter bestimmten Vorraussetzungen vollen Beweis dafür begründet, dass die darin enthaltene Erklärung von dem Aussteller abgegeben wurde. Für Papierdokumente ist diese Echtheitsvermutung in § 416 Zivilprozessordnung (ZPO) geregelt für den Fall, dass das Dokument vom Aussteller unterschrieben oder mit notariell beglaubigtem Handzeichen unterzeichnet wurde. Für elektronische Dokumente ist diese Echtheitsvermutung in § 371a ZPO geregelt unter der Voraussetzung, dass das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen ist. § 371a ZPO findet allerdings nur Anwendung auf originär erzeugte elektronische Dokumente, nicht auf eingescannte Dokumente. Fraglich ist aus meiner Sicht jedoch, ob es einheitlicher Regelungen, die zu einer Echtheitsvermutung auch für eingescannte Dokumente führen, überhaupt bedarf. Die ärztliche Dokumentation in Papierform bedarf keiner Unterschrift, so dass auch diesbezüglich die Echtheitsvermutung des § 416 ZPO nicht gilt. Darüber hinaus wird in der Regel bei der ärztlichen Dokumentation die Frage des Inhalts von Bedeutung sein. In diesen Fällen erfolgt aber sowohl bei Papierdokumenten als auch bei elektronischen Dokumenten die Beweiserhebung mittels Augenschein. Beweisregeln, wie etwa eine

Echtheitsvermutung, gibt es hierfür nicht. Augenscheinsobjekte unterliegen der freien richterlichen Beweiswürdigung nach § 286 ZPO. Es kommt hierbei auf die richterliche Überzeugung an, ob das vorgelegte Dokument den Beweis der Richtigkeit des Inhalts erbringt. Unter welchen Voraussetzungen Gerichte im Rahmen ihrer Beweiswürdigung eingescannten elektronischen Dokumenten welchen Beweiswert zusprechen werden, lässt sich derzeit noch nicht abschließen beurteilen.

Im übrigen wäre für die Schaffung der von Ihnen angesprochenen Regelungen für die Archivierung von Dokumenten in Arztpraxen und Krankenhäusern das Bundesministerium für Gesundheit nicht der richtige Ansprechpartner. Entsprechende Verfahrensregelungen könnten entweder in den Berufsordnungen der Kammern oder den Krankenhausgesetzen der Länder, Beweisregeln in der ZPO, für die innerhalb der Bundesregierung das Bundesministerium der Justiz zuständig ist, festgeschrieben werden.

Allenfalls hinsichtlich der elektronischen Patientenakte gemäß § 291a Abs. 3 Satz 1 Nr. 4 SGB V wäre eine Zuständigkeit des BMG gegeben. Ob es diesbezüglich Regelungen zur elektronischen Archivierung geben wird, steht derzeit noch nicht fest. Die Überlegungen hierzu sind jedoch noch nicht abgeschlossen.

Mit freundlichen Grüßen
Im Auftrag

Schmitt