Norbert Pohlmann

Beweissicherheit in der medizinischen Dokumentation (I)

Im Zeitalter der EDV-gestützten Erstellung, Verarbeitung und Archivierung von Dokumenten stellt sich häufig die Frage nach der Beweissicherheit elektronischer Dokumente. Am Beispiel eines Arztbriefes zeigen wir mögliche Szenarien auf und diskutieren insbesondere die Beweissicherung aus informationstechnischer Sicht.

Damit ein medizinisches Dokument als beweiskräftig gilt, müssen mindestens zwei Dinge feststehen: die Identität des oder der Bearbeiter und die Integrität, also die Unverletztheit, des Dokuments selbst. In diesem Punkt unterscheidet sich die elektronische nicht von der klassischen Archivierung. Und auch die Methoden bzw. Hilfsmittel, mit denen Identität und Integrität überprüft und gewährleistet werden, ähneln einander stark – einschließlich der Probleme, die sie mit sich bringen. Die Rede ist von der eigenhändigen Unterschrift und ihrem Gegenstück, der (qualifizierten) elektronischen Signatur.

Eigenhändig unterschriebene Dokumente

Klassische Archivierungssysteme bieten keinen ausreichenden Schutz vor Manipulationsversuchen

Handgeschriebene Unterschriften erfüllten im Geschäftsalltag bis vor einigen Jahren gleich mehrere Funktionen: Erstens vollendeten sie einen Vertrag oder eine Erklärung und hoben sich daher optisch von deren jeweiligem Text ab. Dies bezeichnen wir als **Abschlussfunktion**. Zweitens stellten sie die Identifizierbarkeit des Ausstellers eines Dokuments sicher (sog. **Identitätsfunktion**). Ob ein Dokument tatsächlich von seinem Unterzeichner stammte, ließ sich drittens durch die Gutachten von Schriftsachverständigen feststellen – die Unterschrift selbst hatte somit eine **Echtheitsfunktion**. Für den Unterzeichner bzw. Aussteller eines Dokuments erfüllt sie eine **Warnfunktion**, da von ihm erwartet wird, dass er den zu unterschreibenden Text auch liest und versteht. Zusammen genommen ergibt sich daraus bei einem Rechtsstreit die **Beweisfunktion** vor Gericht (Urkundenbeweis).

Gerade aufgrund dieser Merkmalkombination und des damit verbundenen hohen Werts in unserem Rechtssystem waren die handgeschriebene Unterschrift und handsignierte Dokumente aber von Anfang an **Ziel von Manipulationsversuchen**. Dabei bedienten sich die Fälscher verschiedener Methoden: Die herkömmlichste darunter ist, das betreffende unterschriebene Dokument (Urkunde) erneut in veränderter Form zu erstellen. Würde der Arzt aus unserem Beispiel einen Arztbrief selbst verändern wollen, müsste er noch nicht einmal seine eigene Unterschrift fälschen. Er benötigt lediglich freien Zugriff auf das Original, um dies durch das veränderte Dokument zu ersetzen.

Dieses Original bleibt in der Regel eine ganze Weile in einer Patientenakte erhalten, bevor es aus Platzgründen auf Mikrofilm untergebracht wird. Während dieses Zeitraums ist es gegen eine Entnahme nicht geschützt. Daneben weist die konventionelle Archivierung folgende Schwachstellen auf, die Paul Schmücker in seinem Buch „Dokumentenmanagement- und Archivierungssysteme“ auflistet:

- Raummangel,
- begrenzte Öffnungszeiten der Archive,
- langes Suchen,
- lange Wegezeiten,
- unterschiedliche Ordnungskriterien,
- begrenzte Zugriffsmöglichkeiten,
- schwieriges Wiederauffinden von Akten aufgrund unzureichender Transparenz (Ordnung bzw. Sortierung der Dokumente innerhalb der einzelnen Akten),
- nachträgliches Eintreffen von Dokumenten.

Angesichts dieser zahlreichen Eingriffsmöglichkeiten und technischen Einschränkungen lässt sich die für juristische Verfahren erforderliche Beweissicherheit bzw. Beweiskraft mit konventionellen Archivierungsmethoden kaum sicherstellen.

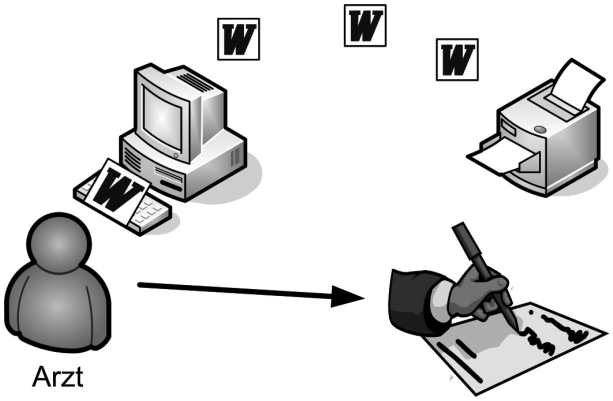

ABB. 1: Traditioneller Entstehungsprozess eines medizinischen Dokuments

Aufgrund zahlreicher Einsparungen im Gesundheitswesen und der Vermehrung elektronisch verfügbarer Patientendaten (Röntgenbilder, EKGs/EEGs, Laborbefunde etc.) ist das Verlangen nach einem elektronischen Archiv entstanden. Ein solcher Wechsel ist aber nur dann sinnvoll, wenn das konventionelle Archiv komplett „digitalisiert“ wird, so dass keine konkurrierenden Systeme entstehen. Zu beachten ist dabei allerdings, dass mit dem Übergang auch neue Manipulationsmöglichkeiten entstehen. Diese möchten wir im Folgenden erläutern und zusätzlich Verfahren vorstellen, die trotz dieser Probleme eine beweissichere Dokumentation ermöglichen.

Elektronische Dokumente

Das gilt ebenso für die einfache elektronische Archivierung, die das Spektrum an Möglichkeiten sogar noch erweitert

Mit dem Wechsel zur elektronischen Datenverarbeitung werden medizinische Dokumente wie Arztbriefe in einem Textverarbeitungsprogramm erstellt und dann entweder lokal auf dem betreffenden Rechner oder aber zentral in einem Datenspeicher abgelegt. Bei dieser elementaren Form der Datenspeicherung entsteht jedoch das Problem, dass sich das Dokument jederzeit aus dem Speicher zurückholen lässt, so dass entweder der Arzt selbst oder Dritte Veränderungen daran vornehmen können. Das äußere Erscheinungsbild ändert sich dadurch nicht; theoretisch wäre es also möglich, nachträglich abweichende oder völlig entgegengesetzte Befunde niederzulegen, ohne dass die gedruckte Version Spuren dieser Manipulation aufweist. Eine weitere einfache Methode besteht darin, das Datum des Computers auf den benötigten Tag einzustellen und dann einfach ein neues Dokument anzulegen, wobei man gleichzeitig andere Versionen löscht.

Um unbemerkte Manipulationen zu erschweren und eine Versionskontrolle zu erleichtern, speichern moderne Textverarbeitungsprogramme wie Word in jedem einzelnen Dokument bzw. jeder Datei so genannte Metadaten ab. Dazu zählen beispielsweise Angaben zum Erstellungsdatum, dem oder den Bearbeiter(n) und dem Zeitpunkt der letzten Veränderung. Auf diese Weise lässt sich nachvollziehen, welcher Autor wann auf ein Dokument zugegriffen hat, seine Kollegen können dies später kommentieren. Per Default werden diese Metadaten dem normalen User zwar nicht angezeigt. Allerdings reichen schon geringfügige Änderungen an den Grundeinstellungen aus, um dies zu ändern. Bei jüngeren Word-Versionen genügt es manchmal sogar, vor dem Öffnen eines Dokuments eine Zeitlang mit dem Mauszeiger darüber zu verweilen, um sie angezeigt zu bekommen.

Obwohl vom Prinzip her also sehr nützlich, bieten Metadaten keinerlei Schutz gegen „nachträgliche Eingriffe“ an einem Dokument. Vielmehr können sie selbst gezielt und vergleichsweise einfach manipuliert werden, wie die zweite oben beschriebene Methode zeigt. Da sich also weder ihre Herkunft eindeutig klären noch ihre Integrität schützen bzw. zweifelsfrei nachweisen lässt, besitzen auf diese einfache Weise abgespeicherte Dokumente vor Gericht keinerlei Beweiskraft.

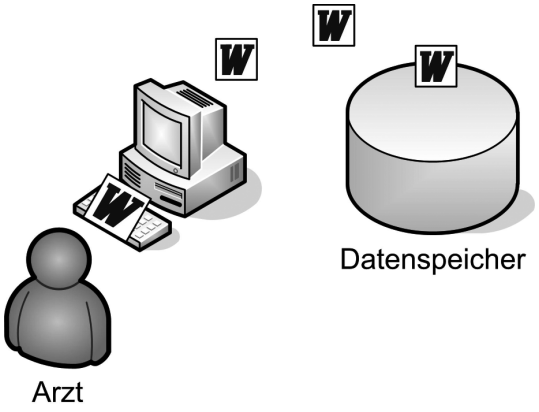

ABB. 2: Entstehung eines elektronischen medizinischen Dokuments (einfachste Art)

Elektronische Signaturen

Aus diesem Grund empfiehlt sich in kritischen Bereichen wie der medizinischen Versorgung die Einführung einer qualifizierten Signatur

Um diese Probleme in den Griff zu bekommen und die Herkunft/Urheberschaft eines Dokuments und der darin enthaltenen Informationen, seinen Bearbeitungsstatus usw. feststellen und nachweisen zu können, ist es daher sinnvoll und notwendig, eine elektronische Signatur einzuführen. Dabei hilft z. B. die **Health Professional Card (HPC),** deren Einführung in absehbarer Zeit auf breiter Front ansteht: Bei diesem Arztausweis handelt es sich um eine SmartCard, welche Schlüssel für eine qualifizierte elektronische Signatur enthält. Hat ihr Inhaber seinen Arztbrief einmal damit signiert, lassen sich hinterher am gesamten Dokument keine unbemerkten Änderungen mehr vornehmen: Fortgeschrittene Archivierungssysteme erzeugen aus der Signatur und dem Inhalt des Dokuments mit Hilfe von Hash-Funktionen einen eindeutigen „Fingerabdruck“ des Dokuments (sog. Hashwert), der ebenfalls abgespeichert und bei dessen Versand zusätzlich übermittelt wird. Andere Benutzer können das Dokument nun unter Verwendung der gleichen Funktion auf seine „Echtheit“ prüfen: Da schon der kleinste nachträgliche Eingriff diesen verändern würde, beweist eine Übereinstimmung beider Hashwerte, dass keine Manipulation stattgefunden hat – und somit die Authentizität und Integrität des kompletten vorliegenden Dokuments.

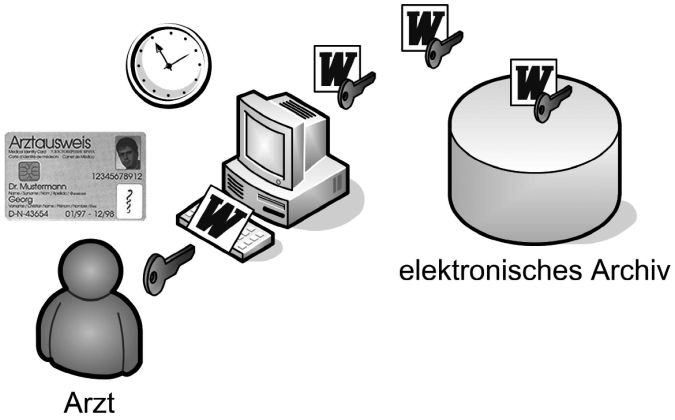

ABB. 3: Elektronisches Archiv für elektronisch signierte Dokumente

Eine weitere Schutzfunktion ergibt sich daraus, dass sich das medizinische Dokument mit Hilfe der für die Signatur eingesetzten Technologie auch für die Übertragung über ungesicherte Transportkanäle verschlüsseln lässt, was die Vertraulichkeit der Datenübermittlung sichert. Und letztlich ist der Arzt bei Verwendung einer HPC gegenüber dem System authentifiziert, was die Verbindlichkeit seiner Dokumentation sicherstellt. An dieser Stelle haben wir einen ähnlichen Grad der Beweissicherheit erreicht, wie sie durch unseren papierbasierten unterschriebenen Arztbrief gegeben ist. Allerdings bleibt auch hier die Frage ungelöst, wie sich das spätere Ersetzen eines Dokuments durch ein anderes feststellen bzw. ausschließen lässt.

Anforderungen an das elektronische Archiv

Daraus ergeben sich besondere Anforderungen an die Datenspeicherung, die eine revisionssichere Archivierung erlauben. Folgende zehn Punkte müssen unbedingt gewährleistet sein:

- Ordnungsmäßigkeit;
- Vollständigkeit;
- Sicherheit des gesamten Verfahrens;
- Schutz vor Veränderung und Verfälschung;
- Sicherung vor Verlust;
- Nutzung nur durch Berechtigte;
- Einhaltung der Aufbewahrungsfristen;
- Dokumentation des Verfahrens;
- Nachvollziehbarkeit und
- Prüfbarkeit.

Im Detail sind die Anforderungen und deren Umsetzung den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) zu entnehmen. Wie diese im Einzelnen aussehen und sich in der Praxis umsetzen lassen, ist Thema der zweiten Folge dieses Beitrags im nächsten Heft.

Zum Autor: Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen.