Überschreibungssicherheit elektronischer Arztdokumente

Sven Thöne, Hannes Federrath
Universität Hamburg
Fachbereich Informatik
Arbeitsbereich Sicherheit in verteilten Systemen

Arbeitspapier, März 2015

Zusammenfassung

Das Patientenrechtegesetz ist in der IT-Healthcare-Branche aktuell in aller Munde, obwohl aus dem Gesetz kaum wesentliche Neuerungen hervorgehen, die an die ärztliche (elektronische) Dokumentation gestellt werden. In diesem Beitrag werden zunächst wesentliche softwaretechnische Mechanismen zur Überschreibungs- und Fälschungssicherheit elektronischer Dokumentationen allgemein diskutiert. Typische Softwaresysteme zur Patientendokumentation, wie sie in Arztpraxen und Krankenhäusern heute Anwendung finden, werden anschließend auf ihre Funktionalität hinsichtlich der Beweiskraft analysiert.

1 Einleitung

Ärzte sind seit 1980 durch ihre Berufsordnung dazu verpflichtet, ihre Patientenakten so zu führen, dass sie auch bei Verwendung elektronischer Systeme nicht nachträglich verändert werden können bzw. dass Änderungen und vor allem Löschungen nachvollziehbar bleiben.

Das Patientenrechtegesetz vom Februar 2013 [1] hat eine neue Diskussion zur Überschreibungs- und Fälschungssicherheit elektronischer Dokumentationen aufgeworfen, denn häufig zweifeln Gerichte an der Korrektheit einer elektronischen Dokumentation, wenn nicht sichergestellt ist, dass diese manipulationssicher ist.

Um Überschreibungs- und Fälschungssicherheit elektronischer Dokumente zu erreichen, müssen entsprechende softwaretechnische Mechanismen in den Softwareprodukten zur Patientendokumentation vorhanden sein. Dabei muss der Schutz nicht nur bei den Eintragungen des Krankenhaus- oder Praxispersonals (z.B. Ärzte, Krankenpfleger, Diagnostik) gewährleistet sein, sondern die Software muss auch vor Angriffen auf das IT-System (z.B. durch bösartiges Personal, Hacker, organisierte Kriminelle) schützen.

Grundsätzlich sind für eine überschreibungs- und fälschungssichere elektronische Dokumentation die standesrechtlichen und gesetzlichen Rahmenbedingungen zu erfüllen, die sich – neben der Musterberufsordnung (MBO) für Ärzte [2] – vor allem aus dem Patientenrechtegesetz (Behandlungsvertrag) in den §§ 630a-f BGB (Bürgerliches Gesetzbuch) ergeben. Insbesondere regelt § 630f BGB, dass Berichtigungen und Änderungen von Eintragungen in der Patientenakte nur zulässig sind, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies gilt auch für elektronisch geführte Patientenakten. Dabei ist zu beachten, dass bei Röntgenbehandlungen zusätzlich der Autor aus der Dokumentation eindeutig hervorgehen muss. Des Weiteren muss eine transparente,

nachvollziehbare Datenverarbeitung (Aufnahme, Speicherung, Veränderung und Übermittlung) wie sie u.a. im Bundesdatenschutzgesetz gefordert wird, durchgeführt werden.

Eine überschreibungs- und fälschungssichere elektronische Dokumentation ist generell nicht nur für die laufende Dokumentation, sondern auch für die Archivierung der Patientenakte (z.B. nach abgeschlossener Behandlung) erforderlich. Dabei besteht zwischen der laufenden und der archivierten Dokumentation eine starke Verbindung: Elektronisch erzeugte Dokumente werden nach ihrer Erstellung üblicherweise zunächst mit einer elektronischen Signatur und/oder einem Zeitstempel versehen, archiviert und in der laufenden Dokumentation wieder verfügbar gemacht.

Die Verbindung zwischen der laufenden und der archivierten Dokumentation ist bei einer teilelektronischen Nutzung (siehe Abschnitt 3) der Dokumentation besonders wichtig, um auch dem Beweiswertverlust nach Medienbrüchen, wie sie bei Transformationen durch Einscannen und/oder Ausdrucken entstehen, vorzubeugen.

Bei der Archivierung werden üblicherweise elektronische Signaturen verwendet, deren Art und korrekte Anwendung in der ZPO (Zivilprozessordnung), SigG (Signaturgesetz) und SigV (Signaturverordnung) geregelt sind.

2 Schutzmechanismen

Überschreibungs- und Fälschungssicherheit in der elektronischen Dokumentation kann nicht allein durch die Datenintegrität, d.h. alle Bits sind unverändert und ungewollte Änderungen werden erkannt, sondern nur durch die sog. Unabstreitbarkeit der Einträge und deren Veränderungen, d.h. die Identität von Zugriffsberechtigten, erreicht werden. Grundlegend muss dafür in der Software ein entsprechendes Rollen- und Berechtigungskonzept vorhanden sein, das nur Personen, die direkt am Behandlungsverlauf des Patienten teilnehmen, einen Zugang zu den sensitiven Patientendaten ermöglicht.

Auf Rollen- und Berechtigungskonzepten setzen die meisten der in diesem Abschnitt diskutierten softwaretechnischen Mechanismen auf, um Überschreibungs- und Fälschungssicherheit zu gewährleisten. Wie Rollen- und Berechtigungskonzepte realisiert werden können, ist z.B. allgemein in [3] beschrieben und nicht Gegenstand dieses Beitrags.

Protokollierung ist eine Möglichkeit, einen eindeutigen Nachweis von nachträglichen Änderungen zu erbringen. Dabei müssen Änderungen benutzerbezogen und automatisch protokolliert werden, ohne dass die Protokollierung beispielsweise vom Krankenhaus- oder Praxispersonal abgeschaltet oder umgangen werden kann.

Protokollierung als Sicherheitsmaßnahme setzt somit auch Vertrauen in den Betreiber des IT-Systems voraus, in dem protokolliert wird. Üblicherweise geschieht die Protokollierung jedoch innerhalb einer Arztpraxis oder eines Krankenhauses. Aus Sicht eines Patienten, der einen Behandlungsfehler mit Hilfe einer Arztdokumentation beweisen möchte, genügt daher die Protokollierung beim Betreiber des IT-Systems alleine nicht, da eine nachträgliche Veränderung der Akte *und* der Protokolle nicht ausgeschlossen ist. Es muss zumindest möglich sein, dem Patienten jederzeit verzögerungsfrei auf seinen Wunsch hin den aktuellen Dokumentationsstand (inkl. der Änderungen und Löschungen) auszuhändigen.

Eine vollständige Protokollierung erfasst das *Wer* (Verfasser), *Wann* (Datum und Uhrzeit) und *Was* (Ergänzungen, Änderungen oder Löschungen) beim Arbeiten an einer Dokumentation. Die Protokollierung findet über die Datenfelder der jeweiligen Objekte (etwa Textfelder, Checkboxen, Auswahlboxen) statt, die in der Software der elektronischen Dokumentation ausgewählt oder ausgefüllt werden können.

Bei Eingaben muss protokolliert werden, was eingegeben wurde. Bei Änderungen muss ersichtlich sein, was geändert wurde. Bei Löschungen muss ersichtlich sein, was gelöscht wurde. Durch die Protokollierung von Datum und Uhrzeit ist aus dem Protokoll eindeutig erkennbar, ob es sich um eine nachträgliche Änderung oder Löschung handelt. Darüber hinaus kann natürlich auch die Benutzeridentität durch die Protokollierung mit erfasst werden; dies ist insbesondere für Röntgenbehandlungen nötig, bei denen der Autor per Gesetz eindeutig aus der Dokumentation hervorgehen muss.

Eine derartige Protokollierung wird üblicherweise bei einer **Datenbankprotokollierung** durchgeführt, die auf dem Rollen- und Berechtigungskonzept aufsetzt und einen Beitrag zur Überschreibungs- und Fälschungssicherheit der elektronischen Dokumentation leisten kann.

Eine noch umfassendere Protokollierung ist mit der **Aktionsprotokollierung** möglich: Sogenannte Audit-Trails setzen ebenso wie die Datenbankprotokollierung auf das Rollen- und Berechtigungskonzept auf und erfassen alle Aktionen und Eingaben der Nutzer, also nicht nur Ergänzungs-, Änderungs- und Löschereignisse, sondern auch Ereignisse wie Lesezugriffe, Druck- und Kopiervorgänge.

Audit-Trails greifen stark in das informationelle Selbstbestimmungsrecht des Krankenhaus- oder Praxispersonals ein, sodass die Beteiligung von Arbeitnehmervertretungen (Personal- und Betriebsräte) sinnvoll und notwendig erscheint. Die Einbindung von Datenschutzbeauftragten ist ohnehin bei allen Fragen der personenbezogenen Dokumentation selbstverständlich.

Versionierung ist eine weitere Möglichkeit, nachträgliche Änderungen erkennbar zu machen. Hierbei wird vor jeder Änderung eine Versionskopie der gesamten oder nur von Teilen der Dokumentation erstellt. Die verschiedenen Versionen werden üblicherweise im Krankenhaus- und Praxisdokumentationssystem revisionssicher abgelegt und in der elektronischen Dokumentation wieder verfügbar gemacht, sodass die einzelnen Versionen einsehbar sind und jede nachträgliche Änderung somit eindeutig aus der Dokumentationshistorie hervorgeht.

Document-State-Machine (Dokumenten-Zustandsmaschine) [4] ist ein dokumentenbezogenes Konzept der Versionierung elektronischer Dokumente. Die Funktionsweise der Document-State-Machine lehnt sich an die von Buchführungssystemen an. Im Gegensatz zur Versionierung wird die Document-State-Machine lediglich zur Erstellung und Bearbeitung von elektronischen Dokumenten eingesetzt, während Versionierung ein eher allgemeines, datenformatunabhängiges Konzept ist.

Bei der Erstellung eines elektronischen Dokuments unter Nutzung der Document-State-Machine wird jedem Dokument nacheinander einer der drei Zustände *erzeugt*, *bearbeitet* oder *abgeschlossen/validiert* zugewiesen. Jedes Dokument muss jeden Zustandsschritt einmal durchlaufen. Setzt ein Arzt das Dokument auf *abgeschlossen/validiert*, ist dies wie eine Unterschrift zu verstehen, sodass keine weiteren Änderungen auf dem erzeugtem Dokument durchgeführt werden können.

Will der Arzt das schon abgeschlossene Dokument stornieren, um beispielsweise Berichtigungen vorzunehmen, wird dies ähnlich wie bei der Versionierung über Kopien (Snapshots) realisiert. Die Snapshots werden revisionssicher archiviert und die Änderungen des Arztes können auf dem Originaldokument vorgenommen werden.

Gelegentlich werden (nicht nur bei einer Document-State-Machine) **elektronische Zeitstempel** und **elektronische Signaturen** eingesetzt, sodass mit einer qualifizierten elektronischen Signatur ein rechtssicheres Dokument mit Urkundencharakter entsteht.

Neben den schon genannten technischen Mechanismen zur Überschreibungs- und Fälschungssicherheit gibt es auch alternative schwächere Varianten, die eingesetzt werden können:

Beispielsweise kann der Arzt wie bei einer papierbasierten Dokumentation verfahren und einfach sein „**Kürzel**“ in der elektronischen Dokumentation hinter den getätigten Eintrag (bzw. die Ergänzung, Kor-

rektur oder Streichung) setzen. Ohne Datenbankprotokollierung oder Audit-Trail kann allerdings bei dieser Variante keine Überschreibungs- und Fälschungssicherheit gewährleistet werden. Zudem ist sie fehleranfällig, da die Kennzeichnungen versehentlich vergessen oder absichtlich weggelassen werden könnten. Sie setzt somit vollständiges Vertrauen in das Krankenhaus- oder Praxispersonal voraus.

Eine weitere Möglichkeit ist die Verwendung eines **digitalen Stiftes** [5], der mit einer Kamera und weiteren Sensoren ausgestattet ist. Der digitale Stift nimmt mit einer Kamera die auf speziellem Papier gemachten handschriftlichen Aufzeichnungen auf und generiert mit Hilfe einer Software daraus ein elektronisches Dokument. In die Metadaten des Dokuments werden dabei Zeitpunkt der Änderung und weitere Informationen (z.B. Haltewinkel, Nutzungsdauer) beigefügt, die der Stift über die Sensoren aufnimmt. Beim digitalen Stift handelt es sich allerdings nicht um einen rein softwaretechnischen Mechanismus, sondern um eine kombinierte Lösung, die aus der Hardware, dem Stift und der entsprechenden Software besteht.

3 Erreichbare Sicherheit der Mechanismen

Um Angriffe auf IT-Systeme zu beschreiben und Gegenmaßnahmen zu identifizieren, werden Angreifermodelle genutzt. Ein realistisches Angreifermodell umfasst dabei nicht nur die momentan zu erwartenden Angriffe, sondern berücksichtigt auch Angriffe, die während der Lebensdauer des Systems in Frage kommen.

Bei Angreifern wird allgemein zwischen Insidern und Outsidern sowie passiven und aktiven Angreifern unterschieden. Der passive Angreifer nimmt eine Beobachterhaltung ein und liest beispielsweise E-Mails aus der Kommunikation im Netz mit. Der aktive Angreifer hingegen verändert Systemzustände. Dabei löscht, verändert oder fügt er Daten ein. Für die Überschreibungs- und Fälschungssicherheit der softwaretechnischen Mechanismen ist der aktive Angreifer interessant, der Veränderungen an den in der Dokumentation enthaltenen Daten vornimmt. Daher betrachten wir passive Angriffe nicht weiter. Wir wollen grundsätzlich von einer vernetzten Einrichtung ausgehen, d.h. die Praxis- bzw. Krankenhausinformationssysteme sind mit dem Internet (oder mit anderen externen Kommunikationssystemen) verbunden. Ein Angriff auf eine unvernetzte Einrichtung kann aufgrund der fehlenden Kommunikationsverbindung nach außen zumindest von Outsidern kaum erfolgreich durchgeführt werden und wird im Folgenden nicht näher betrachtet.

Abbildung 1 hält für vier typische Angreiferrollen,

- zwei Insider, d.h. Arzt/Pflegekraft und Systemadministrator der Arztpraxis bzw. des Krankenhauses sowie
- zwei Outsider, d.h. Patient und krimineller Hacker,

zunächst deren unterstellte Stärke fest und bewertet anschließend, inwieweit die oben genannten softwaretechnischen Schutzmaßnahmen gegen die jeweilige Angreiferrolle schützen.

Veränderungen an den Doumentationen kann ein **Patient** lediglich im Behandlungszimmer durchführen; Voraussetzung hierfür ist, dass der Rechner nicht gesperrt ist. Falls in der Software keine Datenbankprotokollierung oder Audit-Trails als softwaretechnischer Mechanismus integriert sind, kann der Patient eine Veränderung an den Patientendaten vornehmen, ohne dass diese erkannt wird.

Falls eine Datenbankprotokollierung in der Software direkt abschaltbar ist (in einigen Softwareprodukten war dies möglich), können Veränderungen vom **Krankenhaus- oder Praxispersonal** an den Patientendaten unbemerkt vorgenommen werden. Diese Manipulationsmöglichkeit besteht ebenso bei der Vari-

Angreifermodell				
Rolle des Angreifers	Outsider	Insider	Insider	Outsider
Verhalten des Angreifers	aktiv	aktiv	aktiv	aktiv
Technisches Fachwissen	gering	gering	hoch	hoch
Finanzielle Mittel	gering	mittel	mittel	hoch
Rechenkapazität	gering	gering	mittel	hoch
Beispiele für Angreifer	Patient	Arzt, Pflegekraft	System-administrator	Krimineller Hacker

Softwaretechnischer Mechanismus				
Datenbankprotokollierung	○	◖	●	●
Aktionsprotokollierung (Audit-Trail)	○	○	●	◖
Versionierung	○	○	◖	◖
Document-State-Machine	○	○	◖	◖
Elektronischer Zeistempel	○	○	○	◖
Elektronische Signatur	○	○	○	◖
Variante Papierakte („Kürzel“)	◖	◖	●	●
Variante digitaler Stift	○	○	◖	○

Bedeutung der Symbole	
Erfolgreicher Angriff wahrscheinlich möglich	●
Erfolgreicher Angriff eingeschränkt möglich	◖
Keine wahrscheinliche Angriffsmöglichkeit	○

Abbildung 1: Angreiferrollen und Schutzmechanismen im Vergleich

ante Papierakte („Kürzel“), soweit keine nicht abschaltbare Datenbankprotokollierung oder Audit-Trails eingesetzt werden.

Ein **Systemadministrator** oder eine Person mit Administratorrechten verfügt über die nötige Kenntnis und den Zugang, um Veränderungen an Patientendaten vorzunehmen. Die Manipulation kann hier direkt in der Datenbank vorgenommen werden, sodass weder Datenbankprotokollierung noch Audit-Trails oder die Variante Papierakte („Kürzel“) einen Schutz vor Veränderungen bieten. Bei Document-State-Machines und bei der Versionierung bestehen immer noch eingeschränkte Manipulationsmöglichkeiten, sofern dem Angreifer die Speicherformate, Snapshot- und Versionierungsmechanismen ausreichend bekannt sind. Falls elektronische Zeitstempel und/oder Signaturen eingesetzt werden, steigt der Aufwand für den Angreifer weiter. Insbesondere die Sicherheit der elektronischen Signatur beruht auf kryptographischen Verfahren, die selbst durch einen sehr starken Angreifer nicht mehr gebrochen werden kann – die korrekte Implementierung dieser Verfahren vorausgesetzt.

Kriminelle Hacker können Veränderungen an den Patientendaten durch einen Angriff über die Kommunikationsverbindungen nach außen durchführen. Datenbankprotokollierung, Audit-Trails etc. können umgangen werden, indem Veränderungen direkt an der Datenbank erfolgen. Document-State-Machines und Versionierung lassen sich wie beim Systemadministrator u.U. ebenfalls erfolgreich angreifen, da der Angreifer praktisch mit Administratorrechten handelt. Sofern kriminelle Hacker über ausreichend Rechenkapazität verfügen, wäre auch ein erfolgreicher Angriff auf elektronische Zeitstempel und Signaturen denkbar. Wahrscheinlicher als das Brechen kryptographischer Verfahren ist jedoch, dass bisher unerkannte bzw. unbekannte Schwachstellen in den vorhandenen Systemen und Anwendungen (sog. Zero-Day-Sicherheitslücken) von kriminellen Hackern ausgenutzt werden.

4 Nutzungsformen der Dokumentation

Im Folgenden werden am Markt gängige Krankenhaus- und Praxisdokumentationssysteme auf Vorhandensein von Funktionen zur Gewährleistung von Überschreibungs- und Fälschungssicherheit untersucht. Die Untersuchung wurde im Rahmen einer studentischen Masterarbeit [4] an der Universität Hamburg für den Großraum Hamburg durchgeführt.

In Bezug auf die Überschreibungs- und Fälschungssicherheit elektronischer Dokumentationen in Arztpraxen und Krankenhäusern ist vor allem die Nutzungsform der Dokumentation interessant. Je nach Nutzungsform (vollelektronisch, teilelektronisch oder papierbasiert) können softwaretechnische Mechanismen in einer vollelektronischen oder teilelektronischen Dokumentation eingesetzt werden, um die Datenintegrität und mit Einschränkungen auch die Unabstreitbarkeit einer Dokumentation sicherzustellen.

Wir unterscheiden für **Arztpraxen** folgende Nutzungsformen:

1. *Vollelektronisch*: Alle Daten werden in einer elektronischen Dokumentation erfasst und verarbeitet.
2. *Teilelektronisch*: Diese Nutzungsform unterteilt sich in zwei Varianten, die jedoch im Folgenden nur noch wenn nötig unterschieden werden: 2.1 Anteilig teilelektronisch und papierbasiert: Alle Daten werden anteilig in einer papierbasierten und elektronischen Dokumentation erfasst und verarbeitet. 2.2 Parallel teilelektronisch und papierbasiert: Alle Daten werden sowohl papierbasiert als auch in einer elektronischen Dokumentation erfasst und verarbeitet.
3. *Papierbasiert*: Alle Daten werden ausschließlich auf Papier erfasst und verarbeitet.

In Hamburger Arztpraxen wird eine Dokumentation wie folgt genutzt: (n=40) 51 Prozent nutzen die vollelektronische Dokumentation, 42 Prozent nutzen eine teilelektronische Dokumentation und 7 Prozent dokumentieren rein papierbasiert.

Auch für **Krankenhäuser** unterscheiden wir vier Nutzungsformen:

1. *Vollelektronisch*: Von der Patientenaufnahme bis zur Patientenentlassung werden die Daten in der elektronischen Dokumentation erfasst und verarbeitet.
2. *Teilelektronisch*: Auch in Krankenhäusern unterteilt sich diese Nutzungsform in zwei verschiedene Varianten: 2.1 In dieser teilelektronischen Lösung werden die Daten anteilig in einer papierbasierten und elektronischen Dokumentation erfasst und verarbeitet. Im Anschluss an die Entlassung des Patienten aus dem Krankenhaus wird die papierbasierte Dokumentation durch Einscannen mit der schon bestehenden elektronischen Dokumentation zusammengeführt. 2.2 Von der Patientenaufnahme bis hin zur -entlassung wird eine papierbasierte Dokumentation geführt. Im Anschluss an die Entlassung werden alle Dokumente durch Einscannen in eine elektronische Form überführt und verfügbar gemacht.
3. *Papierbasiert*: In dieser Nutzungsform wird ausschließlich eine papierbasierte Dokumentation geführt.

In Hamburger Krankenhäusern wird eine Dokumentation wie folgt genutzt: (n=14) 7 Prozent nutzen die vollelektronische Dokumentation, 79 Prozent nutzen eine teilelektronische Dokumentation und 14 Prozent arbeiten noch rein papierbasiert.

Die Zahlen sind noch einmal in Abbildung 2 zusammengefasst und illustrieren stichprobenartig die Verhältnisse im Großraum Hamburg, sind jedoch nach unserer Auffassung auch bundesweit von Belang.

	Arztpraxen	**Krankenhäuser**
Vollelektronische Dokumentation	51%	7%
Teilelektronische Dokumentation	42%	79%
Papierbasierte Dokumentation	7%	14%
Größe der Stichprobe:	*n=40*	*n=14*

Abbildung 2: Nutzungsform der Dokumentation in den untersuchten Einrichtungen

Aus den Zahlen geht hervor, dass in den Hamburger Krankenhäusern vermehrt ein teilelektronischer Betrieb der Dokumentation genutzt wird. Auch die rein papierbasierte Dokumentation wird in Krankenhäusern noch genutzt. Das ist damit zu erklären, dass Prozessänderungen in Krankenhäusern aufwändiger und kostenintensiver sind. Mit der Überschreibungs- und Fälschungssicherheit hat dies nichts zu tun.

In der Mehrzahl der untersuchten Krankenhäuser wird eine papierbasierte Fallakte – auch Präsenzakte genannt – geführt, die nach dem Verlassen des Patienten eingescannt und über das Krankenhausinformationssystem in elektronischer Form zur Verfügung gestellt wird. Durch das Einscannen der Dokumente (Transformation von einem Papier- in ein elektronisches Dokument) erfährt die Dokumentation einen Medienbruch. Durch den Medienbruch kann der Beweiswert der Papierdokumentation, die Urkundencharakter hat, nicht unmittelbar auf die elektronische Dokumentation übertragen werden. Deswegen werden die Papierakten auch nach dem Scannen weiter aufbewahrt. Auch die elektronische Signatur kann den Beweiswert einzelner Eintragungen in der Akte höchstens mittelbar sicherstellen.

In den Hamburger Arztpraxen ist im Gegensatz dazu inzwischen überwiegend ein vollelektronischer Betrieb der Dokumentation zu finden. Auch die teilelektronische Dokumentation ist häufig anzutreffen. Lediglich ein geringer Anteil der Arztpraxen führt noch eine papierbasierte Dokumentation.

5 Praktischer Einsatz von Schutzmechanismen

Die untersuchten Hamburger Arztpraxen nutzen innerhalb ihres Praxisdokumentationssystems die Datenbankprotokollierung und elektronische Signaturen und/oder Zeitstempel. Die untersuchten Krankenhäuser nutzen darüber hinaus auch Audit-Trails und die Document-State-Machine.

Abbildung 3 gibt einen Überblick über die Ergebnisse. Von den 40 untersuchten Arztpraxen gaben lediglich 12 an, überhaupt softwaretechnische Mechanismen zur Überschreibungs- und Fälschungssicherheit in ihren elektronischen Dokumentationen einzusetzen. In den befragten Krankenhäusern waren es immerhin 11 von 14, die solche Mechanismen einsetzen. Die schwächere Variante („Kürzel“) wurde lediglich in Arztpraxen verwendet. Der digitale Stift wurde in den untersuchten Arztpraxen und Krankenhäusern noch nicht genutzt, obwohl dieser Dokumente erzeugt, die sehr sicher gegen unbefugtes oder unerkanntes Verändern sind und dem Urkundencharakter sehr nahekommen.

	Arztpraxen	**Krankenhäuser**
Anteil der Einrichtungen, die softwaretechnische Mechanismen zur Überschreibungs- und Fälschungssicherheit nutzen	12 von 40	11 von 14
Softwaretechnischer Mechanismus		
Datenbankprotokollierung	8 von 12	7 von 11
Aktionsprotokollierung (Audit-Trail)	0 von 12	2 von 11
Document-State-Machine	0 von 12	1 von 11
Elektronischer Zeistempel oder Signatur	3 von 12	7 von 11

Abbildung 3: Softwaretechnische Mechanismen im praktischen Einsatz

Maximallösungen, die in den Arztpraxen und Krankenhäusern angetroffen wurden, nutzen in der laufenden Dokumentation eine Kombination folgender softwaretechnischer Mechanismen:

- Datenbankprotokollierung und Audit-Trail,
- Document-State-Machine,
- Elektronische Signatur und Zeitstempel.

Im Archiv bzw. in der archivierten Dokumentation wurden folgende softwaretechnische Mechanismen verwendet, um Überschreibungs- und Fälschungssicherheit sicherzustellen:

- WORM-Datenträger (Write Once, Read Multiple),
- Elektronische Signaturen und Zeitstempel.

6 Schlussbemerkungen

Die Analyse zeigt, dass in den untersuchten Krankenhäusern überwiegend ein teilelektronischer Betrieb bei der Dokumentation eingesetzt wird. In den untersuchten Arztpraxen ist die elektronische Datenverarbeitung weiter fortgeschritten als in den untersuchten Krankenhäusern. Hier nutzen über 50 Prozent der Arztpraxen eine vollelektronische Dokumentation.

Je nach Digitalisierungsgrad einer (teil- oder vollelektronischen) Patientenakte können entsprechende softwaretechnische Mechanismen eingesetzt werden, um die Datenintegrität sowie die Überschreibungs- und Fälschungssicherheit der elektronischen Dokumentationen sicherzustellen. Üblicherweise bieten die vorhandenen Krankenhaus- und Praxisdokumentationssysteme mehr softwaretechnische Mechanismen an, als letztendlich von den Einrichtungen genutzt werden. Gerade in Arztpraxen hat sich gezeigt, dass häufig nur eine Datenbankprotokollierung eingesetzt wird, die zumindest vor schwachen Angreifern schützt.

Gerade bei Angreifern mit einer hohen kriminellen Energie kann allerdings durch die alleinige Nutzung von softwaretechnischen Mechanismen wie Datenbankprotokollierung und Audit-Trails unter Umständen keine Überschreibungs- und Fälschungssicherheit in der elektronischen Dokumentation mehr gewährleistet werden.

Bei einigen Softwareprodukten besteht daher noch Handlungsbedarf beim Einsatz von softwaretechnischen Mechanismen, um auch einen Schutz vor starken Angreifern in der elektronischen Dokumentation zu gewährleisten.

Literatur

1. Bundesministerium für Gesundheit: Patientenrechte. http://www.bmg.bund.de/praevention/patientenrechte/patientenrechte.html Abruf am 22.11.2014.
2. Bundesärztekammer: (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (Stand 2011). http://www.bundesaerztekammer.de/page.asp?his=1.100.1143 Abruf am 22.11.2014
3. Alexander Tsolkas, Klaus Schmidt: Rollen- und Berechtigungskonzepte. Springer Vieweg, 2010.
4. Sven Thöne: Überschreibungs- und Fälschungssicherheit elektronischer Dokumentationen in Arztpraxen und Krankenhäusern. Masterarbeit, Universität Hamburg, Fachbereich Informatik, 2014.
5. Mobile Dokumentation: Digitale Stifte und Stifttechnik. http://www.mobile-dokumentation.de/de/digitaler-stift/digitale-stifte-und-stifttechnik/ Abruf am 5.12.2014