Dokumentensicherheit in multimedialen klinischen Informationssystemen

Pharow P[1], Steinebach M[2], Blobel B[1]
[1]*eHealth Competence Center, Klinikum der Universität Regensburg, Deutschland*
[2]*MERIT, Fraunhofer-Institut für Sichere Informationstechnologie Darmstadt, Deutschland*
peter.pharow@eh-cc.de

Einleitung und Fragestellung Das heutige Gesundheits- und Sozialwesen in Deutschland ist entscheidend geprägt von sinkenden Einnahmen und wachsenden Ausgaben. Dabei wachsen parallel auch die Ansprüche der Patienten, denn die vorhandene Technologie erlaubt modernere und bessere Behandlungsmethoden. Ein besonderer Wandel ist hierbei im Hinblick auf die Arten erfasster und gespeicherter medizinischer Daten zu beobachten. Waren bis vor wenigen Jahren noch verbale Informationen und Kodes (SNOMED, ICD, ICPM usw.) charakteristisch für die meisten medizinischen Datensammlungen (Patientenakten, Dokumente), so hat sich das in den letzten Jahren dramatisch geändert. Der Anteil multimedialer Daten (Bilder, Video, Audio usw.) hat permanent zugenommen und wird in naher Zukunft noch weitaus schneller als bisher wachsen. In der Verbindung von medizinischen, Datenschutz- und Sicherheitsaspekten liegt die Herausforderung [1]. Die notwendige Sensibilisierung der recht inhomogenen Nutzer-Community für die wachsenden und gewachsenen Anforderungen an bzw. durch IT-Sicherheit, Datensicherheit und angewandten Datenschutz in der Welt der multimedialen medizinischen Daten beruht im Wesentlichen auf sicheren Verfahren und Lösungen. Sowohl theoretische Grundlagen und Anforderungen als auch praktische Beispiele sollen aufzeigen, wo die neuen Herausforderungen zu finden sind und wie diesen Herausforderungen auf der Basis von bereits existierenden und neuen Lösungen begegnet werden kann. Wissenschaft und Industrie arbeiten hier Hand in Hand, um die Forderungen seitens der Anwender zu erfüllen.

Material und Methoden Speziell für den Bereich des Gesundheitswesens sollen moderne sicherheitstechnische Methoden und Mechanismen für die Speicherung und Archivierung von medizinischen Informationen (Kodes, Daten, Dokumente, Bilder, Audio, etc.) nutzbar gemacht werden. Die gesetzlichen Grundlagen, wie z.B. Sozialgesetzbuch und Röntgenverordnung, schreiben oftmals eine Aufbewahrungsfrist von bis zu 30 Jahren und mehr vor [2]. In all diesen Jahren muss der Inhalt sicher aufbewahrt und gesichert verifizierbar sein. Das erfordert von den eingesetzten Verfahren einen hohen Grad an Robustheit, denn heutige Archivierungssysteme garantieren nicht in jedem Fall die mechanische Speicherung auf Datenträgern wie Mikrofiche, Film, Band, CD oder Festplatte über diesen Zeitraum ohne Umspeicherung oder Umkopierung. Adäquate Mittel der Datensicherheit, wie Signaturen, Zeitstempel und Wasserzeichen, müssen diesen Anforderungen Rechnung tragen. Insbesondere der Aspekt zunehmend durch Geräte unmittelbar erzeugter multimedialer Informationen wurde bisher im Gesundheitswesen oft nur vom Gesichtspunkt der Datensicherung (Backup), nicht aber vom Standpunkt der Datensicherheit und der Integrität der Informationen einschließlich der Nicht-Abstreitbarkeit von Sender und Empfänger auch bei Geräten betrachtet. Neben der Kommunikation der Daten betrifft diese auch und vor allem deren verlässliche Speicherung in Gesundheitsinformationssystemen und Gesundheitsnetzen, elektronischen Archiven und elektronischen Gesundheitsakten (EHR). Jede Art elektronischer Kommunikation zwischen verschiedenen Partnern im Gesundheits- und Sozialwesen setzt ein hohes Maß an Vertrauen voraus. Gerade in dieser Domäne sind auch die Verantwortlichkeit und die Verantwortung für die übermittelten sensitiven Daten besonders hoch. Einerseits erlaubt das heutige System nur dem die Daten erhebenden Arzt die Abrechnung der Leistung gegenüber der Krankenkasse des Versicherten. Somit würde die ungeschützte Weitergabe von Dokumenten (im Sinne der Urheberschaft) jedem Empfänger der Daten ebenfalls diese Möglichkeit eröffnen. Andererseits lässt die Verteilung der rechtlichen Verantwortung des Arztes im Gesundheitssystem heute noch nicht zu, dass Daten anderer Kollegen ohne rechtliche Konsequenzen – vor allem im Falle von Fehler – genutzt werden. Kein Arzt darf durch einen anderen Arzt erhobene Daten bzw. Angaben ohne genaue Überprüfung für die eigene Behandlung nutzen (Beispiel Einholung einer Zweitmeinung). Anders ausgedrückt: hat der übermittelnde Arzt bei der Erhebung der Daten einen Fehler begangen, so ist auch der diese Daten nachnutzende Arzt verantwortlich. Wurden bisher in der Regel echte, als solche erkennbare Kopien an andere Kollegen weiter gegeben, so handelt es sich im Zeitalter digitaler Dokumente häufig in gewissem Sinne um Reproduktionen des Originals. Teilweise ist durch elektronische Medien die Weitergabe von Informationen überhaupt erst möglich geworden (z.B. bei Audiodaten). Aus den genannten Gründen ist die Vermeidung jeglicher Veränderung der Daten eine zwingende Notwendigkeit und somit ein dauerhafter Schutz des unveränderbaren und unveränderten Originals erforderlich [3].

Ergebnisse und technische Perspektiven Der Schutz von Integrität und Authentizität im Bereich digitaler Medien kann auf verschiedene Weisen gewährleistet werden. Dabei ist der Einsatz digitaler Signaturen nur ein erster Schritt, der eine Zuordnung von signierendem Kommunikationspartner (Principal) und Medium sowie im Falle der Übereinstimmung des bei der Signatur des Mediums eingesetzten kryptografischen Hashwertes mit dem aktuell vorliegenden Medien-Hash eine Gewährleistung der Integrität erlaubt. Schwachpunkt der digitalen Signatur ist die fehlenden Lokalisierbarkeit von Manipulationen und das Unvermögen, die Stärke der Manipulation zu bewerten. Fragile digitale Wasserzeichen unterschiedlicher Ausprägung, die speziell zum Integritätsschutz konzipiert worden sind, können diese Probleme lösen. Andererseits sind die meisten Verfahren nicht in der Lage, eine vollständige Garantie hinsichtlich der Integrität der Medien zu liefern. Weiterhin kann durch das Einbetten der Wasserzeichen nicht vermieden werden, dass eine minimale Veränderung der Medien erfolgt. Allerdings können die Verfahren hinsichtlich der Anforderungen optimiert werden, besonders wenn sie direkt in die Prozesskette der Erstellung, Verwaltung und Verbreitung der digitalen Medien integriert werden. So sind beispielsweise steganografische Verfahren bekannt, die bei der Erzeugung digitaler Medien den Kompressionsprozess steuern und somit charakteristische statistische Eigenschaften in den Medien bewirken, ohne dass die Qualität vermindert wird – eine für das Gesundheitswesen unabdingbare Voraussetzung. Es wird lediglich die Entscheidung bei der Zuordnung von Speicherkapazitäten während dem Kompressionsprozess minimal beeinflusst. Ein solches Vorgehen hat den Vorteil, dass nur an einer Stelle der Prozesskette eine Änderung bei der Erstellung der Medien vorgenommen werden muss. Für alle weiteren Schritte ist der Vorgang vollständig transparent, da es sich um einen herkömmlichen Medientyp handelt. Auf diese Weise können beispielsweise inhaltsabhängige Prüfziffern kleinen Bereichen des Mediums zugeordnet werden und später Veränderungen detailliert aufzeigen. Durch Einbetten charakteristischer Merkmale des Originals wird sogar ein Vergleich zwischen Eigenschaften des Originals und der vorliegenden Kopie möglich, ohne dass das Original vorhanden sein muss [4]. Ein weiterer Schritt, der über den Einsatz singulärer Verfahren zum Schutz der Medien hinausgeht, sind Methoden, die unter der Bezeichnung Digital Rights Management (DRM) in erster Linie im Bereich des Urheberrechtsschutzes bekannt sind. Sie vereinen üblicher Weise Methoden zum Gewährleisten von Authentizität und Zugriffsschutz und regeln, welche Rechte bezüglich einer Mediendatei ein Anwender hat. Während im B2C Bereich Kunden oft negativ auf die durch das DRM implizierten Restriktionen reagieren, kann im B2B Bereich oft eine sinnvolle und integrierte Vorgehensweise für DRM gefunden werden, die allen Beteiligten eine effizientere und transparente Handhabe der Medien erlaubt. Die Möglichkeiten gehen hier von einem Sicherstellen des Vorhandenseins einer digitalen Signatur für alle relevanten Medien über einen geschützten Transport der Medien zu allen Beteiligten und eine detaillierte Kontrolle über Zeitraum, Personenkreis und Typ der Nutzung der Medien. Da digitale Medien oft durch Druck oder entsprechende Maßnahmen wieder zu analogen Medien werden, sind robuste digitale Wasserzeichen hier eine sinnvolle Ergänzung der DRM Umgebung, die bei einem Verlassen der geschützten digitalen Umgebung eine Verbindung zwischen Medium und dem für den Vorgang Verantwortlichen ermöglichen, um später potentiellen Missbrauch der Medien verfolgen zu können [5].

Diskussion Die heute installierten elektronischen Informationssysteme, also auch Krankenhausinformationssysteme (KIS) und Bildarchive (z.B. PACS), besitzen keine standardmäßig implementierten Mechanismen zur Gewährleistung der o.g. Anforderungen und können in ihrem Sicherheitslevel durch den Einsatz von Signaturen und Wasserzeichen deutlich verbessert werden. Dabei ist die Zielsetzung eindeutig: Qualitätsverluste jeglicher Art sind aus Gründen der eindeutigen Diagnosestellung nicht akzeptabel, die Daten müssen über lange Zeiträume hinweg technisch lesbar und öffentlich verifizierbar sein. Langzeitsignaturen und andere Mittel sind gefordert, um die rechtliche Verantwortlichkeit auf Dauer zu sichern. Eine Möglichkeit ist das erneute Signieren (Re-Signing) der Daten durch einen unabhängigen Dritten (z.B. Notare), die dann die Verantwortung im Sinne der Signatur für die Unverletztheit des Inhalts übernehmen würden, nicht aber für den unveränderten Inhalt selbst. Dies bedingt die Aufbewahrung der ausgelaufenen Zertifikate über den gleichen Zeitraum wie die Daten selbst. Eine elektronische Gesundheitsakte soll alle relevanten, auf die Gesundheit eines Bürgers bezogenen Daten enthalten, die während des gesamten Lebens erhoben und gespeichert werden. Das erfordert einen hohen Level an technischer und rechtlicher Sicherheit. Zunehmend multimediale Inhalte wie Bilder, Videosequenzen,

Audioaufnahmen, Aufzeichnungen von Geräten wie im Falle von EKG, EEG, EMG, CT, etc. erfordern die Nutzung aller Sicherheitsmechanismen zur Feststellung und Speicherung des Erhebers der Daten (Originator) einschließlich eines gesicherten Zeitstempels sowie eines sehr robusten Wasserzeichens, dessen Verifikation durch Umkopieren oder Umspeichern auch nach vielen Jahren nicht gefährdet werden darf. Gerade im Gesundheitswesen darf in fast allen Szenarien keinerlei Veränderung der Inhalte von Daten (vor allem multimedialer Informationen) akzeptiert werden, da es ansonsten zu Fehlinterpretationen und zu damit zusammenhängenden Qualitätsverlusten der medizinischen Betreuung bzw. auch zu Behandlungsfehlern mit teils fatalen Konsequenzen kommen kann. Es existieren bereits implementierte Lösungen, die bestimmte Teilaspekte abdecken. Weitere Fortschritte sind in nächster Zeit zu erwarten. Die Forschung ist herausgefordert, all die genannten Anforderungen zu erfüllen und gleichzeitig eine Lösung zu präsentieren, die sich nahtlos in alle wichtigen Prozessketten im Gesundheitswesen einbinden lässt.

Literatur

[1] Bake, Blobel, Münch (Hrsg.): Handbuch „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“. datakontext Fachverlag, 2003.

[2] P.Pharow, B.Blobel: Datenschutz im Gesundheitswesen – Ausgewählte Aspekte. In: P. Horster (Hrsg.): D-A-CH-Security 2003 – Bestandsaufnahme und Perspektiven. DuD-Fachbeiträge, Vieweg, Braunschweig / Wiesbaden 2003

[3] P. Pharow, J. Dittmann, B. Blobel: Sicherstellung von Integrität und Verbindlichkeit in digitalen Medien. Informatik, Biometrie und Epidemiologie in Medizin und Biologie Band 34, Heft 3/2003.

[4] Thiemert, Liu, Rauch, Pfannkuche, Fahrion, Steinebach; Digitale Wasserzeichen als Träger von Metainformation für Geographische Informationssysteme - Ein Beitrag im Rahmen des Projektes MediaKomm Esslingen, zfv - Zeitschrift für Geodäsie, Geoinformation und Landmanagement, Heft 5/2004, 129. Jahrgang, pp. 302-305, Wißner-Verlag, ISSN: 1618-8950

[5] M. Steinebach, J. Dittmann, Secure production of digital media, In: M. Hemmje, C. Niederee, T. Risse (Eds.): From Integrated Publication and Information Systems to Information and Knowledge Environments: Essays Dedicated to Erich J. Neuhold on the Occasion of His 65th Birthday. LNCS 3379. Heidelberg: Springer-Verlag, pp. 79-86.