INTEGRITÄT, VERTRAULICHKEIT UND AUTHENTIZITÄT GEWÄHRLEISTEN

Die Digitale Signatur im Gesundheitswesen

In Krankenhäusern, Arztpraxen und anderen Einrichtungen des Gesundheitswesens werden zunehmend die Papierakten und Karteikarten durch elektronische, multimediale Patientenakten ersetzt. Patientendaten sollen auf elektronischem Wege einrichtungsübergreifend und schnell mit mitbehandelnden Ärzten, Kliniken, Reha-Einrichtungen, Apotheken, Pflegediensten etc. ausgetauscht werden. Die elektronische Erzeugung, Langzeitspeicherung und die Übertragung von hochsensiblen Patientendaten, Befunde, Arztbriefe, Rezepte, Diagnosen und Termine wirft zahlreiche Fragen hinsichtlich des Datenschutzes und der Datensicherheit auf.

Von Cornelia R. Vosseler

Damit ergibt sich die Notwendigkeit, neue Sicherheitskonzepte einzusetzen, die die Vertraulichkeit, Integrität und Authentizität der elektronischen medizinischen Dokumentation sowie der Übertragung regeln. Die Partner der Kommunikation müssen sich darauf verlassen können, dass die medizinischen Daten unverfälscht den richtigen Empfänger erreichen (Integrität), dass die Daten nicht von Unbefugten "abgehört" werden können (Vertraulichkeit) und dass sich der Empfänger sicher sein kann, dass die Nachricht wirklich von dem Absender kommt (Authentizität). Dies kann durch sichere Verschlüsselungsverfahren bei der Übertragung und durch die Technik der digitalen Signatur gesichert werden. Für die digitale Signatur wurden die gesetzlichen Grundlagen mit dem novellierten Signaturgesetz, der darauf aufbauenden Signaturverordnung und weiteren Vorschriften im Jahre 2001 geschaffen.

Beweismittel im Haftungsprozess

Untersuchungen in Krankenhäusern zeigen, dass derzeit ca. 50 Prozent der Dokumente in den Papier-Krankenakten handschriftlich unterschrieben und gegengezeichnet werden: von Ärzten, von Patienten, von Pflegekräften, von medizinisch-technischem Personal. Arztbriefe werden üblicherweise von drei Ärzten (Chefarzt, Oberarzt und Untersuchendem/Behandelndem Arzt) unterschrieben, um die Verantwortlichkeit zu zeigen. Damit kommt der digitalen Signatur in einer "papierreduzierten", elektronischen medizinischen Einrichtung eine große Bedeutung zu.
Ein weiterer Aspekt ist, dass Patientenakten in Haftungsprozessen eine entscheidende Rolle als Beweismittel spielen. Die Rechtsprechung kann unter Hinzuziehung von Sachverständigen über die Echtheit, Unverfälschtheit und Vertrauenswürdigkeit entscheiden, ist aber an keine gesetzlichen Beweisregeln gebunden.

Smartcart und PIN

Das übliche technische Mittel zur digitalen Signatur ist die Smartcard, eine kreditkartengroße Plastikkarte mit Chip. Jede unterschriftsberechtigte Person der medizinischen Einrichtung erhält diese mit ihren persönlichen Zugriffsrechten und Identifizierungsdaten - in der Regel eine PIN (persönliche Identifikationsnummer), zukünftig sind auch biometrische Verfahren (z.B. Fingerabdruck, Augenhintergrund) einsetzbar. Damit kann die Smartcard - neben der elektronischen Unterschrift - auch zur Anmeldung (Sign-on) in den Informationstechnologie-Systemen genutzt werden, d.h. die manuelle Passwort-Eingabe kann entfallen. Wünschenswert ist eine Kombination dieser Smartcard mit Mitarbeiterausweis, Zahlkarte für Cafeteria, Zugangskontrollen, Dienstzeitnachweis etc. um den Mitarbeiter fest an eine Karte zu binden.

Für die digitale Signatur enthält die Smartcard zwei Schlüssel, die von einem Zertifizierungsdienstleister (als neutraler vertrauenswürdiger Dritter) erzeugt werden. Der persönliche oder private Schlüssel ist Ersatz für die persönliche Unterschrift und identifiziert den Inhaber, der öffentliche Schlüssel wird vom Zertifizierungsdienstleister in ein öffentliches Verzeichnis aufgenommen und ermöglicht dem Nachrichten-Empfänger den Absender über dieses Verzeichnis zu identifizieren. Für die Datenübertragung von Absender zu Empfänger selbst sind sichere Verschlüsselungsverfahren für die Dateien unabdingbar.

Digitale Signatur hat sich noch nicht durchgesetzt

Die Anwendung der digitalen Signatur in der klinischen Routine hat sich jedoch noch nicht durchgesetzt (siehe "Blitzumfrage zum Einsatz der Digitalen Signatur"). Wesentliche Ursachen sind die Kosten der persönlichen Smartcard, vor allem bei Vergabe durch einen Zertifizierungsdienstleister (so genannte Trust-Center), fehlende performante, nutzer- und prozessgerechte Integration in den vorhandenen Informationstechnologie-Systemen, die unklare Beweislage im Haftungsprozess und die noch ungeklärte Frage der sicheren Langzeitarchivierung digital signierter Dokumente von bis zu 30 Jahren.

BLITZUMFRAGE ZUR DIGITALEN SIGNATUR

Vosseler Consulting befragt KIS-Anbieter

Im April 2003 hat Vosseler Consulting zwölf Hersteller von Krankenhaus-IT-Systemen nach der aktuellen Umsetzung der Digitalen Signatur in ihren Produkten und der Realisierung im Routinebetrieb angefragt.

Hier in Kürze das Ergebnis:

Die Firmen GWI AG, Inovit GmbH und gap GmbH arbeiten an der Umsetzung und haben Pilotprojekte, die derzeit laufen oder in diesem Jahr geplant sind.

GE Medical Systems Information Technologie setzt die Funktionen Single-Sign-On und Befundfreigabe in den Produkten Centricity RIS und Centricity Carddas in Routine ein. Dazu werden in einem Projekt eine klinikeigene persönliche Smartcard eingesetzt und in einem anderen Projekt die von der Landesärztekammer Sachsen herausgegebene HP-Card.

Die BOSS AG setzt in ihrem KIS-Produkt mit einer klinikeigenen Smartcard die Befundfreigabe in einem Krankenhaus in Routine ein; Single-sign-on und Order-Entry sind geplant.

Diese Informationen beruhen auf den Hersteller-Angaben.

Die Umfrage und Recherche erfolgte durch:

Vosseler Consulting - Coaching - Training

www.khsberatung.com
info@khsberatung.com

STAGNIERENDE IT-BUDGETS BEHINDERN DATENMANAGEMENT

Unternehmen haben offenbar ein überzogenes Vertrauen in die Leistungsfähigkeit ihrer Datensicherungsstrategien. Denn IT-Projekte werden nur begrenzt aufgesetzt. Entsprechende Investitionen für Erweiterungen sind vielerorts auch nicht geplant.

Dies ist das Ergebnis einer paneuropäischen Studie über Herausforderungen und Gefahren beim Datenbackup. Das Londoner Marktforschungsinstitut Winmark führte sie im Auftrag von Quantum, einem Anbieter von Datensicherungssystemen, durch.

Von über 150 befragten Unternehmen glauben insgesamt nur 35 Prozent, dass ihre gegenwärtige Speicherarchitektur das in den nächsten Jahren erwartete Datenwachstum bewältigen kann.

Bei den Befragten sind die Speicherinvestitionen in den letzten beiden Jahren trotz des immensen Datenwachstums nicht nennenswert gestiegen. Die Unternehmen rechnen innerhalb der nächsten drei Jahre mit einer Verdoppelung der Datenbestände, allerdings erwarten aber 40 Prozent stagnierende oder sogar rückläufige IT-Budgets. Dabei ist das Datenwachstum stark von der Unternehmensgröße und der Menge der bereits gespeicherten Informationen abhängig.

38 Prozent der befragten Unternehmen mit weniger als 100 Mitarbeitern gaben an, dass ihr IT-Budget ungefähr gleich bleiben wird, gleichzeitig rechnen sie jedoch mit einem Datenzuwachs von 33 Prozent, was die Speichersysteme einem noch stärkeren Druck aussetzen wird. Größere Unternehmen mit über 500 Mitarbeitern gehen eher von steigenden Budgets aus. Sie äußern jedoch die Befürchtung, dass die Investitionen nicht ausreichen werden, um das Datenwachstum tatsächlich zu bewältigen.