Andreas Schurig, Stellvertreter des Sächsischen Datenschutzbeauftragten

Datenschutzrechtliche Gestaltung telemedizinischer Vorhaben

Teilnahme und Teilhabe des Einzelnen am Gemeinwesen ist in einem auf Freiheit orientierten Staat nur möglich, wenn der Einzelne weiß, wer was zu welchem Zweck über ihn weiß. Klare gesetzliche Vorschriften müssen die Datenverarbeitung der öffentlichen Einrichtungen überschaubar machen. Die Verarbeitung personenbezogener Daten darf nur stattfinden, wenn sie geeignet, erforderlich und zumutbar ist, um ein überwiegendes öffentliches Interesse zu sichern. Je tiefer die Persönlichkeit des Einzelnen berührt wird, umso größer muss die Zurückhaltung öffentlicher Datenverarbeitung sein.

Im öffentlichen Gesundheitswesen werden zunehmend Daten automatisiert verarbeitet. Telemedizin eröffnet handfesten medizinischen Fortschritt. Medizin ist zum großen Teil auf Informationsgewinnung angewiesen. Mit deren Hilfe können moderne Technologien der Diagnostik und der Informationsauswertung ein vollständigeres und schnelleres Bild über den Patienten geben.

Von Anfang an gehörte deshalb zu den Aufgaben des wissenschaftlichen Beirates im Rahmen des SAXTELEMED-Projektes – neben der Erstellung eines Evaluierungskonzeptes - die Erarbeitung eines Datenschutz- und Datensicherheitskonzeptes. Ziel dieser Arbeit war es, den Projekten bei der Vertragsgestaltung mit den Generalunternehmern Hilfestellung zu geben, damit Aspekte der Datensicherheit und des Datenschutzes angemessen berücksichtigt werden. Darüber hinaus sollte mit Hilfe der Erfahrungen im Modellprogramm ein allgemeiner Leitfaden zu dieser Thematik entstehen. Die "Empfehlungen für ein Sicherheits- und Datenschutzkonzept" wurden in dieser Form am 24. März 2000 vom wissenschaftlichen Beirat akzeptiert.

Die Empfehlungen gehen ausführlich auf die rechtliche Situation im Rahmen des Modellprogramms ein (Rahmenbedingungen durch Datenschutzrecht, Zivilrecht und Schadensersatzrisiken, Rechtmäßigkeit digitaler Verfahren, Beweisqualität digitaler Dokumente). In einem zweiten Teil werden Vorschläge für Maßnahmen anhand folgender Kriterien gemacht:

Die **Vertraulichkeit** der erzeugten, verarbeiteten, gespeicherten und übermittelten Daten muss gewährleistet sein, d. h. nur Befugte dürfen personenbezogene Daten zur Kenntnis nehmen.

Eine Verletzung der Vertraulichkeit beschneidet den Patienten in seinen Rechten zur informationellen Selbstbestimmung. Aus einer Veröffentlichung von medizinischen patientenbezogenen Daten bzw. durch einen nicht hinreichend unterbundenen Zugang zu diesen Daten wäre der Gesundheitszustand einer Person erkennbar.

Die **Integrität** der erzeugten, verarbeiteten, gespeicherten und übermittelten Daten muss gewährleistet sein, d. h., personenbezogene Daten müssen

Abstract

während der Verarbeitung unversehrt, vollständig und widerspruchsfrei bleiben. Der Behandlungsauftrag in Einrichtungen des Gesundheitswesens umfasst eine sorgfältige Diagnose und Therapie mit dem Ziel der Heilung des Patienten. Die Echtheit, Korrektheit und Vollständigkeit der Daten vor, während und nach der Bearbeitung und Übertragung ist für die Erfüllung des Behandlungsauftrages von großer Bedeutung. Eine Verfälschung oder Unvollständigkeit der Daten kann zu Fehldiagnosen und Fehlbehandlungen führen und somit die Gesundheit und den Heilungserfolg gefährden.

Die **Verfügbarkeit** der erzeugten, verarbeiteten, gespeicherten und übermittelten Daten muss gewährleistet sein, d. h., personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Die zeitgerechte Verfügbarkeit medizinischer Information kann entscheidend sein für eine erfolgreiche Erfüllung des Behandlungsauftrags. Durch nicht rechtzeitig zur Verfügung stehende Daten kann der Patient Schaden erleiden

Die **Authentizität** der erzeugten, verarbeiteten, gespeicherten und übermittelten Daten muss gewährleistet sein, d. h., die Urheberschaft personenbezogener Daten muss jederzeit festgestellt werden können. Erst bei einer eindeutigen Signierung elektronischer Dokumente lässt sich das volle Potential moderner Technologien ausnutzen und für den Arzt und den Patienten rechtssicher gestalten.

Die **Revisionsfähigkeit** der erzeugten, verarbeiteten, gespeicherten und übermittelten Daten muss gewährleistet sein, d. h. es muss festgestellt werden können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Für den Arzt bzw. das Krankenhaus besteht die Pflicht zur Dokumentation. Daraus ergeben sich Vorschriften zur Archivierung und Archivierungsdauer, forensische Konsequenzen sowie der Nachweis über Negativbefunde usw. Die Frage, wer welche Diagnose und welche Therapie verordnet hat, muss nachvollziehbar bleiben.

Da im sächsischen Telemedizinprojekt digitale Bilddokumente und Befunde sowohl zwischen internen als auch externen Partnern übermittelt, gespeichert und verarbeitet werden sollten, ergaben sich neue Anforderungen an die eingesetzte Technik und Organisation. Reichte bisher die papierne schriftliche Dokumentation samt der Unterschrift des Arztes und der verschlossene Umschlag aus, um die Echtheit und die Vollständigkeit einer Patientenakte zu gewährleisten, so ist dies heute auf andere Art und Weise zu sichern. Diese Notwendigkeit, die sich nicht nur aus Datenschutz und Haftungsansprüchen ergibt, sondern in erster Linie medizinische Gründe hat, führt klar zum Einsatz einer elektronischen Signatur.

Diese sollte in den folgenden Anwendungen verwendet werden:

- Zugangskontrolle zu den Systemen der beteiligten Krankenhäusern und Praxen,
- Befundfreigabe in der Radiologie,
- Informationsübermittlung zwischen den verschiedenen Standorten der Projektpartner.

Abstract

Erleichternd für die Entscheidung zum Einsatz der digitalen Signatur war der Umstand, dass im medizinischen Bereich bereits eine ausgearbeitete Spezifikation für eine Karte vorliegt, die die digitale Signatur gewährleistet, die sogenannte "Health Professional Card (HPC)". Die Arbeitsgruppe des wissenschaftlichen Beirates des Telemedizinprojektes, an der auch die Sächsische Landesärztekammer beteiligt ist, optierte von Anfang an für die grundsätzliche Ausrichtung an dieser Spezifikation. Entscheidungskriterium ist allerdings die Erfüllung der Anforderungen des Signaturgesetzes (SigG), denn nur so ist auch zukünftig die Gleichstellung mit der schriftlichen Dokumentation und damit die von den Ärzten verlangte Rechtssicherheit für elektronische Dokumente gegeben. Da die damals vorhandene HPC-Spezifikation noch nicht in allen Punkten den Anforderungen des Signaturgesetzes (sowohl alter als auch neuer Form) entsprach und in einigen Bereichen auch nicht mit den angebotenen Kartenlösungen der Trust-Center kompatibel war, hatten wir aus den oben genannten rechtlichen Gründen der Erfüllung der Anforderungen des SigG den Vorrang gegeben, wobei jedoch bereits in der Pilotphase sowohl optisch wie technisch eine weitgehende Annäherung an die HPC-Spezifikation angestrebt war.

In drei der acht Teilprojekte des sächsischen Telemedizinprogramms war geplant, die HPC einzusetzen:

Modellprojekt 5	<p>Das Modellprojekt 5 besteht aus zwei unabhängigen Kreiskrankenhäusern der Regelversorgungsstufe. Sie arbeiten medizinisch zusammen in einem virtuellen Verbund, der beispielhaft für die Kooperation der Krankenhäuser der Regelversorgung untereinander in Sachsen stehen kann.</p> <p>Das technologische Konzept zur Umsetzung des HPC-Projekts basiert auf einer modularen Systemarchitektur, in der die Hochrüstung der drei HPC-Anwendungen separat in den jeweils betreffenden Systemen erfolgt. Die Systeme sind mit Standardschnittstellen unter einander verbunden. Dadurch bleibt die unabhängige Nutzbarkeit der hochgerüsteten Systeme erhalten. Die niedrigste Modularitätsebene ist in der Radiologie der PACS Arbeitsplatz. Im PACS werden jeweils die einzelnen Arbeitsplätze zur Befundung und Betrachtung hochgerüstet und bleiben auch nach der Hochrüstung mit den HPC Anwendungen als Einzelsysteme nutzbar.</p>
Modellprojekt 6	<p>Das Modellprojekt 6 besteht aus einem Krankenhaus der Schwerpunktversorgung, drei unabhängigen Krankenhäusern der Regelversorgungsstufe und weiteren niedergelassenen Ärzten, die in einem virtuellen Verbund medizinisch zusammenarbeiten. Es steht beispielhaft für die Kooperation von Krankenhäusern der Regelversorgung und Praxen mit einem Kompetenzzentrum.</p> <p>Das technologische Konzept zur Umsetzung des HPC-Projekts basiert auf einer modularen Systemarchitektur, in der die Hochrüstung der drei HPC-Anwendungen separat in den jeweils betreffenden Systemen erfolgt. Die Systeme sind mit Standardschnittstellen unter einander verbunden. Dadurch bleibt die unabhängige Nutzbarkeit der hochgerüsteten Systeme erhalten. Die niedrigste Modularitätsebene ist in der Radiologie das PACS. Die HPC relevanten Hochrüstungen erfolgen auf dem zentralen PACS-Server.</p> <p>In diesem Modellprojekt wird ergänzend zu den 3 HPC-Anwendungen auch noch die HPC gestützte Langzeit-Archivierung eingeführt und in verschiedenen Kooperationsmodellen getestet.</p>
Modellprojekt 7	<p>Im Modellprojekt 7 sind zwei Kreiskrankenhäuser eines gemeinsamen Trägers zu einem virtuellen Verbund integriert, das beispielhaft für die Integration von Krankenhäusern eines gemeinsamen Trägers stehen kann.</p>

Abstract

	Das technologische Konzept zur Umsetzung des HPC-Projekts basiert auf einer zentralen Systemarchitektur für die Zugangskontrolle, in der die Hochrüstung auf einem speziell dafür eingerichteten Server durchgeführt wird. Dadurch wird erreicht, dass ein Nutzer einmal angemeldet auch gleichzeitig in den anderen Systemen angemeldet ist.
--	---

Der veranschlagte quantitative Umfang des Karteneinsatzes ergibt sich aus folgender Tabelle:

	HPC Sichtausweis + A+B(1+2)+C	Chipkarte für medizin. Personal (A+B2+C)	Chipkarte für medizin. Personal (A)	Summe Karten
Projekt 5	115	40	80	235
Projekt 6	180	50	140	370
Projekt 7	126	34	31	191
ingesamt	421	124	251	796

(HPC - Sichtausweis mit Bild, Name, Kammerzugehörigkeit; A = Authentifizierung (eindeutige Identifizierung des Arztes im EDV-System); B1 = Digitale Signatur bei Befundfreigabe; B2 = Digitale Signatur zur Unterschrift beliebiger Schreiben; C = Schutz von Patientendaten bei ihrer Übertragung in offenen Systemen (Verschlüsselung))

Der HPC-Einsatz startete am 1. Juni 2001. Der weitere Ablauf sollte sich folgendermaßen gestalten:

Adaptionen der Anwendungen an Routinetauglichkeit und Anwenderakzeptanz beim Hersteller	Q3 2001
Vollausbau aller Anwendung nach den Adaptionen	Q3 2001
Klinischer Betrieb & Auswertung / Evaluierung	Q3/Q4 2001

Bereits vor dem Start ergaben sich vor allem organisatorische Probleme. Das Signaturgesetz geht in seiner Grundkonzeption davon aus, dass der einzelne Nutzer einen Vertrag mit einem Trustcenter schließt, das ihm eine Karte mit der Funktionalität digitale Signatur übergibt und – solange der Nutzer zahlt – den Verzeichnisdienst pflegt. Externe Dritte spielen nur dann eine Rolle, wenn es um die Einrichtung und Bestätigung zusätzlicher Attribute geht. Nicht im Blick ist der Umstand, dass beim Einsatz der Karte auch dieser externe Dritte möglicherweise eine rechtsverbindliche Beziehung mit dem Nutzer eingehen will. Dies kann zum einen darin liegen dass der Einsatz der digitalen Signatur gerade an die Attributeigenschaft gebunden ist (z. B. zur Unterschrift berechtigter Beamter) oder eine zusätzliche Funktionalität hinzukommt (Sichtausweis). Der überwiegende Teil der bisher angedachten Einsatzmöglichkeiten der (im neuen SigG qualifizierten) digitalen Signatur sind aber solche Anwendungen (die HPC als Sichtausweis der Ärztekammer, der ministeriale Dienstaussweis, die Bürgerkarte einer Kommune). Damit ergeben sich bisher rechtlich noch unbefriedigend gelöste Fragen: Wer gibt die Karte aus? Wer ist über den Verlust zu informieren? Kann die Karte eingezogen werden? Wer bezahlt?

Der derzeit in Sachsen vorgeschlagene Weg für die HPC sah folgendermaßen

Abstract

aus:

- Der Arzt stellt persönlich unter Vorlage seines Personalausweises einen Antrag zur Ausstellung einer Signaturkarte vom Typ HPC über einen zertifizierten Weg beim Signaturanbieter.
- Die Sächsische Landesärztekammer prüft, ob der Antragsteller Arzt ist und gibt die Herstellung der Signaturkarte vom Typ HPC beim Signaturanbieter frei.
- Der Signaturanbieter generiert die HPC und den PIN-Brief auf zertifizierten Wegen.
- Der Arzt bestätigt den Empfang der HPC dem Signaturanbieter. Dieser informiert die SLÄK.

Ein weiteres – aber besser lösbares – Problem ergibt sich daraus, dass Institutionen Karten mit einem unterschiedlichen Funktionsumfang einsetzen wollten (z. B. Zugangskontrolle), die nicht notwendigerweise mit digitaler Signatur verbunden sind, diese jedoch aber auch umfassen können. Dies führt dazu, dass man im Krankenhaus z. B. drei unterschiedliche Kartentypen einsetzt: die HPC als Sichtausweis mit qualifizierter digitaler Signatur für den Arzt, die Karte mit qualifizierter digitaler Signatur für nichtärztliches Personal mit Unterschriftsberechtigung (z. B. medizinisches Personal oder Buchhaltung) und Karten mit einfacher digitaler Signatur für sonstige Mitarbeiter, bei denen Zugangsberechtigungen überprüft werden müssen. Alle drei sollen möglichst die gleiche Hardware und Software nutzen. Dies stellt hohe Anforderungen an die Organisationskunst der Krankenhausverwaltung und Systembetreuung.

Den wirklich herben Rückschlag erlitt das HPC-Projekt allerdings durch die Tatsache, dass das hinter dem Trustcenter und dem Signaturanbieter stehende Unternehmen diesen Geschäftszweig mitten in der Ausrollphase einstellte. Zwar sind mittlerweile die beschafften Zertifikate wieder verwendbar, eine weitere Beschaffung von Zertifikaten ist jedoch nicht möglich, da der Signaturanbieter, mit dem der Vertrag abgeschlossen wurde, seinen Geschäftsbetrieb eingestellt hat. Der Vorgang ist bedauerlich, macht aber deutlich, dass auch in diesem Bereich ein unternehmerisches Risiko (für alle Beteiligten) besteht, das man bei der Auswahl eines geeigneten Signaturanbieters berücksichtigen muss. Wir haben dies getan und uns entschlossen, einen zweiten Anlauf zu nehmen. Für eine Startphase werden wir das bisherige Ausgabemodell verwenden, dauerhaft soll allerdings die Sächsische Landesärztekammer die Funktion der Zertifizierungsautorität übernehmen.

Damit liegen in der Zukunft noch mehrere Aufgaben vor uns:

- die Einbindung der digitalen Signatur in die Softwareanwendungen
- die Gestaltung einer dauerhaften Ausgabelösung
- die Evaluation der organisatorischen und physischen Kartennutzung

Auch denken wir – optimistisch wie wir sind – auch vor dem Hintergrund der derzeitigen Entwicklung im Gesundheitswesen, vor allem der Einführung der Gesundheitskarte, über eine Einbeziehung dieser Aspekte in unser Projekt nach. Als wir uns vor dreieinhalb Jahren grundsätzlich für die Einbeziehung der HPC entschieden, war diese Intention noch kein Allgemeingut. Mittlerweile hat uns die Entwicklung bestätigt, denn die moderne Telemedizin wird ohne digitale Signatur nicht denkbar sein.