Datenschutz und IT-Sicherheit der Telematik im Gesundheitswesen

Prof. Dr. Klaus Pommerening, Universität Mainz

Einleitung

Wir sind auf dem Weg in die Informationstechnik nicht aufzuhalten. Ärztenetze und Telematikplattformen für die Medizin schießen überall aus dem Boden; überall wird an mehr oder weniger fortgeschrittenen Pilotprojekten gearbeitet. Diese Vernetzung soll die Versorgung der Patienten vereinfachen, verbessern und ökonomisch optimieren, die Wissenschaft fördern und dem Arzt den schnellen und kostengünstigen Zugriff auf für seine Tätigkeit notwendige Informationen bieten.

Bei aller Euphorie - die ich durchaus teile, ich wirke ja selbst auch an Telematikprojekten im Medizinbereich mit - werde ich heute eine sehr pessimistische Sicht vor Ihnen ausbreiten und hoffe, die Diskussion damit anzuregen. Dabei wird es auch Widersprüchlichkeit geben - nicht weil ich nach fünf Minuten nicht mehr weiß, was ich gesagt habe, sondern weil das Thema voller Widersprüche, Interessenskollisionen und Zielkonflikte steckt. Diese müssen gegeneinander abgewogen werden, und das geht nur, wenn alle Probleme und Standpunkte auf dem Tisch liegen.

Das Thema »Patientendaten im Netz« kann man von verschiedenen Gesichtspunkten aus kritisch beleuchten:

- Wohl des Patienten,
- Datenschutz,
- Ökonomie,
- Sicherheitstechnik.

Verschiedene Interessen ringen miteinander, die der

- Patienten, die geheilt werden wollen,
- Ärzte, die heilen und dabei möglichst wenig mit fachfremden Aufgaben belastet werden wollen,
- Kostenträger, die die Versorgung mit den vorhandenen, immer viel zu knappen Ressourcen sichern wollen,
- Wirtschaft, der Hersteller, Netzbetreiber, Informationsanbieter, ..., die Systeme verkaufen und Dienste anbieten und damit Gewinn erzielen wollen,
- Politiker, die das Nötige möglichst publikumswirksam in die Wege leiten wollen.

4. Gesichtspunkt: IT-Sicherheit

Die globale Informationstechnik ist - wie jede Großtechnik - nicht wirklich beherrschbar, der GAU ist oft nur einen Mausklick entfernt. Der menschliche Faktor bleibt z. B. immer ein Risiko. Was schief gehen kann, wird irgendwann einmal schiefgehen: Das ist nicht nur Murphys Gesetz, sondern auch die Lehre aus 15 Jahren Risks-Forum [http://http://catless.ncl.ac.uk/Risks/]. Beispiele aus jüngster Zeit (aus dem Heise-Newsticker [http://www.heise.de/newsticker/]:

- Klinikum rechts der Isar (Labordaten im WWW),
- Kaiser Permanente (Mails mit medizinischen Ratschlägen an die falschen Adressen verschickt),
- Advance Bank (um auch ein Beispiel aus dem vermeintlich so sicheren Bank-Bereich zu nennen - vier Tage lang Zahlungsaufträge zwar angenommen, aber nicht ausgeführt).

Im Bereich der Informationstechnik ist der Vergleich mit der industriellen Revolution des 19. Jahrhunderts durchaus angebracht: Die daraus resultierenden Umweltprobleme werden bis heute nicht beherrscht, im

Gegenteil, sie nehmen trotz Fortschritten bei Einzelaspekten insgesamt immer noch zu.

Die vielfältigen Überlegungen zum Thema »Sicherer Zugriff auf elektronische Patientenakten« sind zwar im wesentlichen korrekt, seriös und technisch realisierbar - aber nur, wenn die Technik *fehlerfrei konzipiert* ist, *fehlerfrei funktioniert* und *fehlerfrei angewendet* wird. Ein äußerst fragiles Gebilde! Sicherheit gehorcht dem Gesetz der Kette: Ihre Wirksamkeit wird durch das schwächste Glied bestimmt.

Vertrauen in einzelne Sicherheitsmaßnahmen ist daher in der Regel naiv. So ist z. B. die durch die VPN-Technik gegebene kryptographische Verschlüsselung auf der Netz-Ebene nicht geeignet, die ärztliche Schweigepflicht gegenüber dem Netzbetreiber zu gewährleisten. Außerdem setzt sie hohes Vertrauen in die Sicherheit des Kommunikationspartners voraus - dessen Sicherheitslücken werden nämlich importiert. Auch die HPC schützt nicht davor, dass in Word-Dokumenten versteckte vertrauliche Daten oder Makroviren transportiert oder Tunnel durch Firewall-Systeme gebahnt werden.

Das Kräftefeld so vieler diverser und teils gegensätzlicher Interessen verhindert konsequente, perfekte Lösungen. Es wird immer nur unvollkommene Kompromisse geben. Notwendigerweise entstehen Löcher, Durchschlüpfe, Tunnel, ... Die sehr empfindliche, unstabile Sicherheit leidet als erstes. Ein Beispiel für solche Instabilität ist die Firewall-Technik - so kann etwa keines der existierenden Systeme einen ernsthaften Untertunnelungsversuch verhindern.

Einige aktuelle, besonders brennende Sicherheitsprobleme will ich nennen:

- Denial-of-Service-Angriffe = Angriffe auf die Verfügbarkeit von Systemen sind im Netz ein Kinderspiel. (Die berühmte Ausfallsicherheit des Internet bezieht sich nur nur auf die Transportebene, nicht auf Dienste.)

- Download von Software außerhalb der Nutzerkontrolle spielt eine immer größere Rolle - vom ständigen Software-Upgrade im Hintergrund bis zu aktiven Inhalten auf WWW-Seiten.

- Jeder Missetäter, Terrorist, Desperado, Erpresser oder Psychopath auf der ganzen Welt ist nur einen Mausklick entfernt.

- Immer mehr Schadprogramme geistern um die Welt; die Verbreitungsmöglichkeiten werden immer einfacher.

- Die Sicherheit der Standard-Software, die auch im medizinischen Bereich überall eingesetzt wird, nimmt immer weiter ab. Gründe dafür sind die rasant wachsende Komplexität (»Featuritis«), die immer mehr Möglichkeiten für Lücken eröffnet, und die große Gleichgültigkeit für Sicherheitsfragen insbesondere beim weltweiten Marktführer im Softwarebereich.

- Die Außerhausgabe von IT-Dienstleistungen (Outsourcing), insbesondere Fernwartung durch Spezialisten, die irgendwo auf der Welt sitzen, lässt Daten kaum noch kontrollierbar um die Welt kreisen.

Wir sind weiter entfernt von einer »ordnungsgemäßen« Datenverarbeitung als je zuvor. Wer mir widersprechen will, muss mindestens nachweisen, dass er keine MS-Produkte einsetzt.

Aber auch die perfekteste Sicherheitstechnik kann nur einen Teil der Probleme lösen. Sie wird immer wieder versagen - nicht weil sie schlecht, sondern weil sie extrem empfindlich und instabil ist. Ein umfassendes Sicherheitsmodell mit stets sicheren Rückfallpositionen ist für kein Anwendungsgebiet der Telematik in Sicht.

3. Gesichtspunkt: Ökonomie

Zum ökonomischen Gesichtspunkt kann ich hier wenig Originelles beitragen.

Natürlich kann (und soll!) Telematik die Qualität der Informationen und der Versorgung verbessern. Vor allem soll sie Kosten senken - und kann das langfristig vielleicht auch.

Die Informationstechnik leistet aber sicher nur einen Teil dessen, was Optimisten sich von ihr versprechen, dafür kostet sie erheblich mehr an Zeit und Geld als erhofft. Nur an wenigen Stellen kann sie kurzfristig Zeit oder Geld sparen - unbestreitbar spart sie Postlaufzeiten und, wenn die Netze und Rechner denn mal amortisiert sind, auch Portokosten.

Die Telematik erhöht jedenfalls das Tempo und den ökonomischen Druck (das ist ja so gewollt!) und kann damit dem medizinischen Prozess durchaus schaden.

2. Gesichtspunkt: Datenschutz

Der eigentliche Angriff auf die Persönlichkeitsrechte mit Hilfe der Informationstechnik steht noch vor uns - aber sehr nah. Die Zustände in den USA lassen ahnen, was alles nicht mehr zu verhindern ist, wenn die Daten erst einmal elektronisch vorhanden sind. Z. B. kann der verbreitete Handel mit Kundendaten auch Handel mit Patientendaten sein (Surfprofile bei der Suche nach medizinischen Informationen u. dgl.). Informationen, die einmal entschlüpft sind, lassen sich nicht wieder einfangen. Die freie Kopierbarkeit von Daten ist nicht einschränkbar. Wie ist eigentlich das »Vergessen« im Netz geregelt? Wie kontrollierbar? Global?

Ein Land, das sich hohe Datenschutzanforderungen und ein hohes Sicherheitsniveau leistet, ist auf dem Weltmarkt nicht konkurrenzfähig. Als Folge dieses Effekts ist ein globales Einpendeln auf dem niedrigsten Niveau zu erwarten.

Die universelle, verteilte Patientenakte ist nicht wirklich zu schützen - nicht auf Dauer, nicht weltweit und nicht vor kommerziellen Verwertungsinteressen. Und natürlich auch nicht vor totalitären Regimes. Man stelle sich vor, zur Zeit Nationalsozialisten hätte es die elektronische Patientenakte schon gegeben. Die unbedingte Vertraulichkeit der Patientendaten verbietet dem Arzt, sie einer Technik anzuvertrauen, die er nicht selbst unter Kontrolle hat. Die verteilte elektronische Patientenakte kann er nicht unter seiner Kontrolle haben!

Und schließlich kann der Datenschutz in telematischen Systemen nicht besser sein, als die Sicherheitstechnik, auf der er beruht.

1. Gesichtspunkt: Interessen des Patienten

Schon gar nicht ist die informationelle Selbstbestimmung des Patienten wirksam aufrecht zu erhalten, wenn seine Daten erst einmal im Netz sind. Er ist dem informationstechnischen Medizin-Apparat ausgeliefert, alles was er sagt, kann gegen ihn verwendet werden.

Das Vertrauensverhältnis des Patienten zum Arzt ist extrem empfindlich und instabil. Welcher Patient vertraut schon seinem Arzt wirklich? (Umgekehrt ist das auch fraglich.) Das kollektive Vertrauen in eine Gruppe - die Ärzte - oder gar eine Maschinerie - das Gesundheitswesen - klappt erst recht nicht. Wir müssen also ausgehen von

\+ Misstrauen gegenüber dem einzelnen Arzt,
++ Misstrauen gegenüber der Ärzteschaft,
+++ Misstrauen gegenüber dem Medizinapparat.

Die einzige Waffe des entmündigten Patienten ist die Verweigerung; je größer sein Misstrauen gegen Arzt und Medizinapparat ist, desto mehr wird er sich mit Angaben zurückhalten, desto schwerer wird es, ihm zu helfen.

Die Entpersönlichung, Entfremdung des Heilungsprozesses schreitet fort. Was der Medizin vor allem anderen fehlt, sind nicht - oder nur in Ausnahmefällen - Daten, sondern es fehlt Zeit, und die wird immer knapper. Die persönliche Beschäftigung mit dem Patienten, die Empathie des Arztes sind nicht durch Informationstechnik zu ersetzen, sondern brauchen Zeit und Ruhe. Die Arbeitsbelastung der Mediziner wird aber durch Informationstechnik nicht verringert; im gleichen Zug, wie mehr Informatiker benötigt werden, werden Mediziner eingespart oder als Systemverwalter und -techniker fachfremd eingesetzt. Oder hat jemand etwas anderes beobachtet?

Handlungsbedarf und Perspektiven

Über Grundanforderungen an die informationstechnische Sicherheit und die Methoden, vor allem kryptographischer Art, zu ihrer Erfüllung, brauche ich in diesem Kreis wohl nichts mehr zu sagen. Die Grundfunktionen Verschlüsselung, digitale Signatur, starke Authentisierung beruhen alle auf kryptographischen Techniken und werden dem Nutzer bei minimaler Belästigung durch leistungsfähige Chipkarten wie die Health Professional Card (HPC) zur Verfügung gestellt - möglichst bald!

Die HPC ist aber nur ein Stein im Mosaik der informationstechnischen Sicherheit. Äußerste Sorgfalt bei der Konzeption und beim Betrieb von Systemen im Gesundheitswesen ist nötig, eine umfassende Technikfolgenabschätzung, eine ständige Diskussion der Verlässlichkeit. Allerdings fürchte ich, dass der betuliche Ansatz der Technikfolgenabschätzung immer hinter den schon eingetretenen Folgen herhinken wird.

Die Hersteller und Anbieter sind zu defensivem Systemdesign, Schaffung sicherer Rückfallpositionen, Redundanz in Sicherheitsmaßnahmen, zur Konsolidierung und Qualitätssicherung der Software aufgerufen. Sichere Systeme folgen dem KISS-Prinzip: Keep It Small and Simple.

Übrigens ist der Vergleich mit der Sicherheit im Bankbereich trügerisch: Dort sind die Aufgaben, Strukturen und Informationen wesentlich schlichter als im Gesundheitswesen, und es geht um materielle Werte, die einer Kosten-Nutzen-Kalkulation unterliegen und deren Verlustrisiko durch eine Versicherung abgedeckt werden kann. Im Gesundheitswesen dagegen sind Persönlichkeitsrechte zu schützen, deren Verlust oft nicht wieder gutzumachen ist.

Bei aller notwendigen Gründlichkeit hemmt das Warten auf zu perfekte Lösungen aber auch den Fortschritt; die technischen Grundlagen sind schon seit gut zwanzig Jahren vorhanden - dass sich die flächendeckende Nutzung so lange verzögert, spricht für die organisatorische Komplexität der realen Welt: die Zeitdauer der Einführung einer Telematikplattform für die Medizin, der Einführung einer Sicherheitsinfrastruktur. Statt dessen wird immer noch ein neues Projekt gestartet, ein neues Aktionsforum gegründet, das verzweifelt versucht, den Überblick über die Entwicklung zu gewinnen, eine neue Risikoanalyse verlangt, ... Daher z. B. der Rat: PGP und SSL sofort anwenden, die HPC, sobald verfügbar. Es sollte ein Kompromiss zwischen zügiger Einführung von Sicherheitsmaßnahmen und der gründlichen Vorbereitung der perfekten Lösung gefunden werden. Verschlüsselte E-Mail verschicken kann man auch ohne HPC und großen organisatorischen Aufwand.

Die informationelle Gewaltenteilung ist meiner Meinung nach am besten zu verwirklichen, wenn der Patient an der Zugriffskontrolle über seine Daten beteiligt wird, natürlich unter Berücksichtigung von Vorkehrungen für den medizinischen Notfall. Freiwilligkeit und Selbstbestimmung müssen für Patient und Arzt gewährleistet bleiben.

Misstrauen und kritische Einstellungen zur Telematik sollten nicht abgewiegelt oder diskreditiert, sondern ernst genommen werden! Das ist ja auch eines der Grundprinzipien unserer Staatsform.

Wenig kritisch ist die Nutzung der Telematik zur Informationsbeschaffung, wenn genügende Sicherheitsvorkehrungen beachtet werden. Wenn aber Patientendaten im Netz kommuniziert und gespeichert werden sollen, dann nur mit der bestmöglichen Sicherheit nach dem Stand der Technik, insbesondere mit starken kryptographischen Verfahren. Bedenken gegen die Kommunikation im Rahmen eines Behandlungzusammenhangs können so meiner Meinung nach ausreichend gemildert werden. Meine Vorbehalte gegen die Schaffung einer netzübergreifenden elektronischen Patientenakte sind aber nicht so leicht zu zerstreuen.