Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
www.datenschutzzentrum.de/

Dies ist unser Webangebot mit Stand 27.10.2014. Neuere Artikel finden Sie auf der überarbeiteten Webseite unter www.datenschutzzentrum.de.

Vertraulichkeitsschutz durch IT-Sicherheit bei der elektronischen Gesundheitskarte

Dr. Thilo Weichert

Landesbeauftragter für den Datenschutz Schleswig-Holstein,
Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD)

BSI-Kongress 10. bis 12. Mai 2005

- Die begleitenden Vortragsfolien zu diesem Vortrag als PDF-Datei

I. Keine überstürzten Entscheidungen

Im Anfang 2004 in Kraft getretenen Gesundheitsmodernisierungsgesetz ist vorgesehen, dass die elektronische Gesundheitskarte von Anfang 2006 an flächendeckend in der Bundesrepublik eingeführt wird. Inzwischen ist der Zeitplan nicht mehr ganz so ehrgeizig: Selbst die Bundesgesundheitsministerin dürfte eingesehen haben, dass 2006 allenfalls mit der schrittweisen Einführung begonnen werden kann. Bis alle Bürgerinnen und Bürger die Karte haben, wird es noch einige Zeit dauern. Der **ehrgeizige Zeitplan** hat zweifellos seinen Zweck gehabt. Er bewirkte politischen, technischen und wirtschaftlichen Druck auf alle Beteiligten, ihren Beitrag zur gemeinsamen Einführung zu leisten und sich bei den vielen nötigen Abstimmungsprozessen zu einigen. Dennoch darf die flächendeckende Einführung nicht überstürzt werden. Die Einführung neuer Technologien lässt sich nicht politisch oder gesetzlich verordnen, da hierbei ein komplexes Verfahret stattfinden mit technischen, sozialen und kulturellen Komponenten. Dies gilt generell, erst recht aber für ein derart anspruchsvolles Projekt wie die elektronische Gesundheitskarte, bei dem höchst sensible Daten in einer großen Telematik-Infrastruktur verarbeitet werden sollen, an der Tausende äußerst heterogener Parteien beteiligt sein sollen.

Die elektronische Gesundheitskarte kann zum Prototyp für den Aufbau einer komplexen IT-Infrastruktur werden, die funktioniert und zugleich den Anforderungen an ein **IT-Verfahren in einer demokratischen und freiheitlichen Gesellschaft** genügt: Ein demokratisches Verfahren verlangt, dass alle Beteiligten in einem ergebnisoffenen diskursiven Prozess ihre Interessen einbringen können. Voraussetzung für ein freiheitliches Verfahren ist, dass die Grundrechte der Beteiligten gewahrt werden. Betroffene Grundrechte sind zunächst der Schutz der ökonomischen Rechte der Berufsfreiheit und des Eigentums. Dies sind aber auch die informationellen Rechte der Informationsfreiheit und des Vertraulichkeitsschutzes. Die Wahrung dieser Rechte und ein demokratisches Entscheidungsverfahren sind Grundbedingungen für gesellschaftliche Akzeptanz. Und diese Akzeptanz ist wiederum ein absolutes KO-Kriterium bei Verfahren, die auf die aktive Mitwirkung der Bevölkerung angewiesen sind. Ohne die aktive Mitwirkung der Ärzteschaft, sämtlicher Heilberufe und vor allem der Patientinnen und Patienten wäre die elektronische Gesundheitskarte von Anfang an zum Scheitern verurteilt.

II. Vier mahnende Beispiele

Diese banal klingende Erkenntnis ist in der Praxis alles andere als banal: Bei fast keinem der **großen bundesweiten IT-Projekte** aus so unterschiedlichen Ressorts wie Verkehr, Finanzen, Wirtschaft oder Inneres wurde und wird diese Erkenntnis ausreichend berücksichtigt.

- Bei der bundesweiten Einführung der **LKW-Maut** erfolgte weder eine Beteiligung der Betroffenen noch eine präventiv angelegte Technikfolgenabschätzung. Das Ausschreibungsverfahren war undurchsichtig, die

abgeschlossenen Verträge sind es bis heute. Die hochkomplexe IT-Infrastruktur erwies sich als nicht grundrechtskompatibel und musste im Nachhinein nachgebessert werden. Da aber die technischen Vorgaben nicht mehr disponibel waren, musste man sich mit rechtlichen und organisatorischen Vorkehrungen behelfen. Tatsächlich wurde mit dem TollCollect-Verfahren eine umfassende Straßenverkehrs-Überwachungsinfrastruktur aufgebaut, die ein unbeobachtetes Nutzen von Autobahnen fast unmöglich macht. Dass zunächst selbst die Funktionsfähigkeit nicht sichergestellt war, zeigt, dass wichtige Regeln für die vernünftige Einführung eines neuen IT-Systems unbeachtet blieben.

- Ähnlich vernichtend muss die Einführung der **Kontoevidenz** im Bankenbereich bewertet werden: Eingeführt wurde das Verfahren nach der Salamitaktik, erst als Instrument zur Terrorismusbekämpfung und zur Geldwäschebekämpfung, dann zur Förderung der Steuerehrlichkeit gegenüber Finanzämtern und schließlich zur Kontrolle bei sämtlichen staatlichen Finanzbeziehungen, also insbesondere bei der Erbringung von Sozialleistungen. Der parlamentarische Entscheidungsprozess erfolgte im Schnellverfahren in de facto nichtöffentlichen Ausschusssitzungen. Weder die Banken noch die Kontoinhaber wurden irgendwie einbezogen. Einer vorläufigen verfassungsrechtlichen Überprüfung hielt das Verfahren nur Stand, weil ganz kurzfristig mit Hilfe eines Erlasses nachgebessert wurde. Das technische Verfahren ist bis heute nicht transparent, obwohl es seit 1. Mai im Betrieb sein sollte. Die Reaktion hierauf sind gesellschaftliche und politische und rechtliche Widerstände, die voraussichtlich, wenn inzwischen keine Nachbesserung vom Gesetzgeber erfolgt, vor dem Bundesverfassungsgericht sicher Erfolg haben werden.

- Den Sturm der Entrüstung noch vor sich hat das geplante **JobCard-Verfahren**, bei dem die Daten über sämtliche Einkommenszahlungen und evtl. gar sämtlicher Entgeltersatzleistungen sämtlicher abhängig Beschäftigter in Deutschland in einer großen Datenbank abgespeichert werden sollen, um das lästige Ausstellen von Lohnbescheinigungen und Ähnlichem durch die Arbeitgeber und Sozialbehörden zu vermeiden. Positiv dabei ist der Vorlauf mit mehreren Erprobungsstadien im Interesse technischer Machbarkeit. Desaströs ist aber auch hier das völlig Ausblenden jeglicher Technikfolgenabschätzung, was - ohne bösen Willen zu unterstellen - zu einer gewaltigen verfassungswidrigen Vorratsdatenverarbeitung führt. Statt nun das Ergebnis einer Untersuchung der Machbarkeit der von den Datenschutzbeauftragten vorgeschlagenen Ende-zu-Ende-Verschlüsselung abzuwarten, hat das Bundeswirtschaftsminsiterium nun für Herbst ohne Not einen Gesetzentwurf auf der alten technischen Basis angekündigt.

- Vorläufg letztes abschreckendes Beispiel ist die Einführung **biometrischer Ausweisdokumente**. Nach den Anschlägen vom 11. September 2001 gesetzlich beschlossen, bestehen bis heute noch keine konkreten Vorstellungen von der technischen Umsetzung. Bis heute gibt es weder ein Datenschutzkonzept noch ein Sicherheitskonzept. Zumindest mir ist auch kein Finanzierungs- und kein Implementierungskonzept bekannt. Eine Erprobung im Realbetrieb hat nicht stattgefunden. Notwendige gesetzliche Anpassungen sind bis heute nicht erfolgt. Dennoch meint das Bundesinnenministerium, den elektronische Biometriepass zum Herbst dieses Jahres einführen zu müssen. Zudem entstand durch die Ausladung eines Kritikers auf der heutigen Veranstaltung der unschöne Eindruck, dass eine kritische demokratische Auseinandersetzung mit dem Projekt unerwünscht ist. Ob letztendlich eine verfassungsverträgliche Lösung gefunden wird, steht derzeit noch in den Sternen.

  Die vier aufgeführten Beispiele lassen folgende Schlüsse zu: Nur durch ein **geregeltes Ablaufverfahren** lassen sich große Fehlinvestitionen und finanzielle Fehlentscheidungen vermeiden. Die Erprobung eines geplanten Systems mit Korrekturmöglichkeit in jedem Verfahrensstadium ist unabdingbar - nicht nur im Interesse der Funktionalität, sondern auch der Demoraktieverträglichkeit. Dabei muss eine ergebnisoffene öffentliche Debatte stattfinden. Schließlich kommt der Grundrechtsverträglichkeit eine zentrale Bedeutung zu. Jedes der genannten IT-Verfahren kann eine grundrechtsgefährdende, ja evtl. gar grundrechtsprengende Wirkung entfalten. Betroffen sind so unterschiedliche Rechte wie das Recht auf unbeobachtete Mobilität oder die Vertraulichkeit der Banken-Kunden-Beziehung durch umfassende wirtschaftliche Kontrolle oder allgegenwärtige Identifizierungspflichten.

  Ein zentraler Aspekt bei modernen IT-Projekten ist der **Vertraulichkeitsschutz**. Der Mensch soll sich – insbesondere bei den alltäglichen Verrichtungen - darauf verlassen können, dass er selbst

bestimmen kann, wer was bei welcher Gelegenheit über ihn weiß, d.h. dass seine Daten vertraulich behandelt werden. Das Bundesverfassungsgericht hat klargestellt, dass unser Grundgesetz vom Leitbild des informationell selbst- und nicht fremdbestimmten Bürgers ausgeht. Dieses Leitbild besteht nicht nur im individuellen Interesse der Menschen, sondern liegt auch im Gemeinwohlinteresse, "weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratisches Gemeinwesens ist" - so das Bundesverfassungsgericht.

III. Die Bedeutung der Vertraulichkeit medizinischer Behandlung

Was für die Nutzung der Autobahn, die Kundenziehung zu Finanzdienstleistern, für die Einkommensverhältnisse und für Identifizierungspflichten aus Sicherheitsgründen gilt, das gilt erst recht für den Medizinbereich. Die Vertraulichkeit der **Arzt-Patienten-Beziehung**, das Patientengeheimnis ist Grundbedingung für den Heilerfolg: Wer befürchtet, dass seine Behandlungsdaten an Dritte weitergegeben werden, wird sich überlegen, ob er dem Arzt die für die Behandlung nötigen Informationen offenlegt. Auch hier bekräftigte das Bundesverfassungsgericht, dass dieser Schutz nicht nur im individuellen Interesse des Patienten liegt, sondern, dass dies "im Ganzen gesehen, der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient".

Dabei sollten wir uns keinen Illussionen hingeben: Der Medizinbetrieb zu Beginn des 21. Jahrhunderts unterscheidet sich von der ärztlichen Behandlung zu Zeiten des Hippokrates, 400 Jahre vor Christus und auch fast ebenso zu Zeiten der Begründung der modernen Medizin vor über hundert Jahren. Die Behandlung erfolgt heute hochgradig **arbeitsteilig** und mit großem **bio- und informationstechnischen Aufwand**. Umso wichtiger ist es, die Vertraulichkeitszusage des hippokratischen Eides normativ und technisch umzusetzen.

Arbeitsteilung und Technisierung bedingen zwangsläufig **Datenauswertungen**, von denen man sich vor 30 Jahren noch keine Vorstellungen machte: Dies begint mit der Vergütung medizinischer Leistungen, findet seine Fortsetzung in komplexen Praxis- und Krankenhausinformationssystemen mit der Notwendigkeit automatisierter Wirtschaftlichkeits- und Qualitätskontrolle, in der Auswertung der Patientendaten für Zwecke der Weiterentwicklung von Pharmaprodukten, ärztlichen Behandlungsmethoden und medizinischer Erkenntnis und endet in völlig neuen Informationsbedürfnissen des Patienten selbst, für den im Informationszeitalter medizinische und informationelle Selbstbestimmung eben auch bedeutet, dass er umfassend Kenntnis erlangen kann über Blut- und Leberwerte, über genetische Dispositionen und gesunde und krankhafte Stoffwechselabläufe. Aber auch jenseits des Informationsinteresses des Patienten lässt sich kaum etwas Vernünftiges vortragen gegen Disease Management Programme, integrierte Versorgungskonzepte, wissenschaftliche Kompetenznetzwerke und Krankheits-, z.B. Krebsregistrierungen. Selbst bei der Abrechnung mag es - trotz aller datensparsamen Alternativkonzepte - nicht ganz ohne DRGs und ICDs gehen. Es hat schon immer knappe Ressourcen im Gesundheitswesen gegeben. Deren gerechte Verteilung ist aber in einer Zeit immer weiter gehender technischer Machbarkeit immer mehr auch Aufgabe autmatisierter Datenverarbeitung geworden.

Insofern sind die Pläne für eine elektronische Gesundheitskarte fast zwangsläufig. Ebenso zwangsläufig ist es, deren Funktionalität nicht auf einen Behandlungsausweis zu beschränken, sondern diesen in ein **umfassendes Telematikkonzept** einzubinden, das mit vielen Funktionalitäten aufwartet: Rezeptierung, Medikationskontrolle, Notfalldatenvorhaltung, Behandlungsdokumentation, Patientenaktenverwaltung durch den Patienten selbst. Wir befinden uns in einer großen, technologisch bedingten Umbruchsphase. Ein Weg zurück zum allzuständigen Hausarzt kann es - im Interesse bestmöglicher Versorgung - nicht geben, so wichtig ein solcher Arzt auch als Gesundheitslotse ist.

Diese Erkenntnis ist in der Ärzte- und in der Patientenschaft noch ausreichend nicht angekommen. Beide Gruppen sind von Ängsten geplagt. Diese Ängste betreffen zwei Fundamente ärztlicher Behandlung, nämlich **Autonomie und Diskretion**. Nicht ganz ohne Grund befürchten Ärzte wie

Patienten, dass ihnen mit der Automation Wahlfreiheit und Vertraulichkeit beraubt werden, dass sie Objekte staatlicher Zwangsbehandlung werden könnten. Die Gründe für diese Furcht sind mit Händen zu greifen. So hat die Gesundheitsministerin in den letzten Jahren wohl schon Dutzende Gesetze aufgelegt, deren vorrangiges Ziel es ist, das Behandlungsverhalten der Ärzte für Politik, Gesundheitsverwaltung und Krankenkassen transparenter und kontrollierbarer zu machen. Befürchtet wird zudem staatlicher Dirigismus. Der Lipobay-Skandal gab die Initialzündung für die elektronische Gesundheitskarte genutzt, die Gesundheitsministerin wollte mit der Karte eine obligatorische Medikationsüberwachung der Patienten erreichen. Betrachtet man zusätzlich die im SGB V angelegten Pläne der Klassifikation der Patientinnen und Patienten nach Morbiditätsfaktoren, so scheinen schlimme Befürchtungen von Kranken und Gesunden nicht aus der Luft gegriffen.

IV. Die Regelungen zur elektronischen Gesundheitskarte

Doch muss ich der Gesundheitsministerin etwas bescheinigen, was im Bundeskabinett keine Selbstverständlichkeit ist: Sie zeigte sich lernfähig im Hinblick auf die technische Machbarkeit bestimmter Kontrollvisionen und im Hinblick auf die Grundrechtssensibilität der geplanten Prozeduren. Und so kann man zumindest den **Regelungen zur elektronischen Gesundheitskarte** als Datenschützer bescheinigen, dass sie in fast jeder Hinsicht wohl durchdacht sind und die Bedürfnisse nach Wahlfreiheit und Vertraulichkeit zu befriedigen versuchen: Abgesehen vom eher administrativen Massen-Verfahren der elektronischen Rezepterstellung und -einlösung und der bisherigen Kostenabrechnung werden sämtliche, insbesondere die medizinischen Anwendungen in die Disposition des Patienten unter autonomer ärztlicher Anleitung gestellt. Nicht zu leugnen ist, dass auch bei diesen "Zwangsverfahren" sensible Patientengeheimnisse verarbeitet werden. Die Funktionalitäten, bei denen es um detaillierte Inhalte und Qualität der Behandlung geht, werden aber der Freiwilligkeit der Betroffenen überlassen.

Diese programmatischen Vorgaben technisch umzusetzen ist alles andere als trivial. Schon der erste Schritt hierzu - die gesetzestechnische Umsetzung - zeugt von einer **hohen Komplexität** mit vielen **praktischen Konfliktlagen**: So soll die Autonomie des Patienten dadurch gestärkt werden, dass ihm - auch in technischer Form - umfassend Auskunft über die zu seiner Person gespeicherten Daten erteilt wird. Zugleich aber ist es Realität, dass der Betroffene das schwächste Glied in einer Behandlungskette ist: ihm die Bestimmungsmöglichkeit über seine Patientendaten zu geben, bedeutet ihn den Einflussnahmen von interessierten Kreisen auszuliefern, vom Arbeitgeber über Versicherungen bis hin zu Pharmaunternehmen und Krankenkassen. Nicht einfach zu lösen ist die Aufgabe, die für eine Lebenssituation relevanten Daten verfügbar zu machen, aber auch nur diese. Zudem sollen dem Patienten Wahlrechte zugestanden werden, gegenüber bestimmten Empfänger Daten freizuschalten, gegenüber anderen dagegen das Patientengeheimnis zu wahren. Diese Wahlrechte müssen einem Patienten vermittelt werden, der hiermit oft intellektuell überfordert sein wird. Sein vorrangiges Interesse liegt nicht in der Wahrung seiner Patientenautonomie, sondern in der Sicherung und Wiederherstellung seiner Gesundheit. Des Weiteren muss die Umsetzung der Wahlrechte technisch abgebildet werden. Die Daten des Patienten vertrauensvoll in die Hände eines Arztes, z.B. des Hausarztes zu legen, kann auch nur bedingt sinnvoll sein, zumal auch dieser kaum technische Kompetenz aufweist und zumindest in Bezug auf die Abrechnung diametral andere Interessen verfolgt als der Patient.

Angesichts solcher Konfliktlagen konnte sich der Gesetzgeber bei der Schaffung der Rechtsgrundlagen für die elektronische Gesundheitskarte nicht auf materiell-rechtliche Regelungen beschränken. Er musste sich vielmehr selbst Gedanken über die **technische Umsetzung** machen. Auch insofern gilt dem Gesetzgeber ein großes Lob: Er hat grundrechtlich Wesentliches der Technikgestaltung geregelt und technische Details offen gelassen. So werden z.B. Die Identifizierung per Lichtbild beschrieben, die zulässigen Datenfelder, die Krankenversicherungsnummer. Zitat aus § 291 Absatz 2a SGB V: "Sie (die Karte) muss technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen." Geregelt wird die Authentisierungemethode mit den sog. Health Professional Cards bzw. den elektronischen Institutionenkarten, den sog. Secure Module Cards, geregelt sind die maximale Zahl der Zugriffsprotokollierungen und ein differenziertes Zugriffskonzept. Benannt werden schließlich die

Prozeduren, nach denen die technischen Standards im Rahmen der Selbstverwaltung entwickelt und gesetzt werden sollen. Vor deren Genehmigung ist der Bundesbeauftragte für den Datenschutz zu beteiligen.

Damit ist etwas Außergewöhnliches gelungen: In einem Gesetzentwurf wurden Politikern äußerst vernünftige technische Vorschläge gemacht, die diese auch tatsächlich übernahmen. Dies ist angesichts der schon fast notorischen Technikferne der Politik verblüffend. Praktisch wird im Rahmen der Gesetze das gesamte **technische Datensicherheitsinstrumentarium** bei der Realisierung der elektronischen Gesundheitskarte verordnet: Verschlüsselungsverfahren, die Nutzung unterschiedlicher Pseudonyme, virtuelle private Netzwerke, Verweisverfahren, der Einsatz digitaler Signaturen, differenzierte Zugriffsregelungen.

V. Die Ohnmacht des Patienten

Die Logik der Regelungen zur elektronischen Gesundheitskarte ist vielen noch nicht bewusst, noch mehr wollen sie nicht wahrhaben: In Ergänzung zu materiellen Regelungen zum Schutz von Wahlfreiheit und Vertraulichkeit wird auf technischen Schutz gebaut. Wenn die sensiblen Patientendaten auf der Karte, in der Arztpraxis, auf vielen dezentralen Servern und dort in verschiedenen Postfächern und Rechnersegmenten gespeichert werden, gelten nicht mehr nur die Regelungen des fünften Sozialgesetzbuches und des ärztlichen Standesrechts, sondern vor allem die Gesetze der Informatik. Das Vertrauen in den Arzt muss damit erweitert werden auf das **Vertrauen in Technik**.

Die damit verbundene Erwartung gegenüber Normalverbrauchern, wie es einfache Patientinnen und Patienten sind, ist eine gewaltige Zumutung. Begegnet der Durchschnittspatient doch trotz aller Medien- und Computerbegeisterung der Informationstechnik mit Respekt und Skepsis. Dies gilt insbesondere dort, wo er nicht selbst Agierender ist, wie z.B. bei der Nutzung des Computers im Internet, sondern **reines Objekt der Verdatung**. Und an diesem Umstand können auch die patientenfreundlichsten Regelungen zur elektronischen Gesundheitskarte nichts ändern: Die Generierung der Daten erfolgt durch den Arzt. Wegen der ärztlichen 10jährigen Dokumentationspflicht hat der Patient keine Befugnisse zur Veränderung, Berichtigung oder Sperrung. Allenfalls eine Art Gegendarstellung wäre rechtlich möglich. Eine Einflussnahme auf die Arzt-, Kassen-, Krankenhaus- oder Apothekensysteme ist dem Patienten ebenso wenig möglich wie auf die Telematik-Netzstruktur. Dies gilt für die Systemarchitektur allgemein, für die eingesetzten Programme, für die gewählten Sicherheitsmaßnahmen, ja selbst für die konkrete Dateneingabe bzw. Datennutzung. Subjekt ist der Patient allenfalls bei Auskunftserteilung im Rahmen der Wahrnehmung der Wahlrechte, d.h. bei der Bestimmung der zulässigen Datenempfänger. Ob aber diesen Vorgaben gefolgt wird, entzieht sich schon wieder der Kontrolle des Patienten.

Kann der Patient zumindest über den Bildschirm am Frontend, d.h. in der Praxis oder in der Apotheke, noch verfolgen, was mit seinen Daten passiert, so ist er im Hinblick auf sämtliche **Hintergrundsysteme** den Vorgaben Dritter ausgeliefert. Auf welchen Servern seine Patientendaten gespeichert werden, wo diese stehen, wer dafür verantwortlich ist, welche Zugriffe darauf möglich sind, all das entzieht sich dem Patienten ebenso wie die Beauftragung Dritter durch Arzt, Krankenhaus oder Kasse: Wer wird beauftragt, welche Technik wird eingesetzt, welche Sicherheitsmaßnahmen werden ergriffen?

Das Misstrauen gegenüber den am Telematiksystem anonym bleibenden Beteiligten ist nicht ganz unbegründet: Weiß der Patient doch, dass an der ihn betreffenden Datenverarbeitung sehr viele ein großes **ökonomisches Interesse** haben: Die Krankenkassen zielen nicht nur auf optimale Behandlung ab, sondern auch auf Reduzierung der Gesundheitskosten. Ärzten geht es legitimerweise vorrangig darum, mit der Behandlung Geld zu verdienen. Völlig undurchsichtig sind für den Patienten abgeleitetere Interessen, etwa die der Internet-Apotheken, die im Konflikt stehen zu den Apotheken an der Straßenecke. Selbst vielen beteiligten Spezialisten dürfte kaum klar sein, welche unterschiedlichen Interessen z.B. unterschiedliche Hersteller von Arztpraxissoftware verfolgen, oder welche Interessen und Strategien diese mit Pharmaunternehmen verbinden, für die

z.B. ein Verordnungsmonitoring durchgeführt wird. Die jeweilige technische Lösung der Praxis- oder der Krankenhaussoftware bestimmt mit, ob bestimmte Schnittstellen zu Standardprogrammen zugelassen oder ausgeschlossen werden, ob bestimmte Datenauswertungen möglich sind oder nicht.

Eines ist klar: Die Patientinnen und Patienten wurden zu keinem Zeitpunkt gefragt, ob sie die elektronische Gesundheitskarte wollen. Prognosen zeigen, dass Einspareffekte insbesondere bei der Krankenkassen erreicht werden können. Die großen Verdiener werden aber die IT-Anbieter sein. Bei der Neuverteilung der **Gesundheitskosten** werden diese sich einen größeren Anteil von Gesamtkuchen abschneiden können. Es ist daher nicht verwunderlich, wenn mancher Arzt- und mancher Patientenvertreter die Verhältnismäßigkeit des Mitteleinsatzes in Frage stellt. So mag es z.B. bisher mit den alten GKV-Karten durch unberechtigte Kartennutzung einen gewissen wirtschaftlichen Schaden gegeben haben. Ich habe aber Zweifel, ob dies die großen Kosten rechtfertigt, die allein dadurch entstehen, dass auf die elektronische Gesundheitskarte mit viel technischem Aufwand ein elektronisch gespeichertes Lichtbild aufgebracht wird. Die Kosten von Karte und technischer Infrastuktur müssen letztlich sämtliche von der Solidargemeinschaft getragen werden. Daher hat diese Solidargemeinschaft auch einen Anspruch zu erfahren, welche Kosten auf sie zukommen und wie diese gerechtfertigt werden.

Das zentrale Instrument, mit dem die informationelle und medizinische Selbstbestimmung der Versicherten realisiert werden soll, ist die **Freiwilligkeit** der medizinischen Anwendungen, die daher auch künftig unter keinen Umständen aufgegeben werden darf. Diese Freiwilligkeit hat einen segensreichen Effekt auf die technische Gestaltung und das Sicherheitskonzept: Wollen die Betreiber der Telematik-Anwendungen große Patientengruppen von der Patientennützlichkeit ihrer Angebote überzeugen, und nur dann macht deren Realisierung ökonomisch Sinn, so müssen diese sinnvoll und vertrauenswürdig erscheinen. Der praktische Erfolg der elektronischen Gesundheitskarte wird also wesentlich davon abhängen, dass patientenfreundliche Lösungen gefunden werden.

VI. Eine neue Rolle der Sicherheitstechnik

Zunächst einmal gilt es, die hochsensiblen Daten von 80 Millionen Versicherten bei 300 Krankenkassen, inklusive 8 Millionen Privatversicherte in ein Netz einzuspeisen, an dem neben den Krankenkassen bzw. Krankenversicherungen 130.000 ambulante Arztpraxen, 20.000 Apotheken, 54.000 Zahnärzte und viele andere Heilberufe beteiligt sind. Über dieses Netz sollen nicht nur jährlich ca. 740 Millionen elektronische Verordnungen abgewickelt werden. Es sollen Arzneimittelverträglichkeiten in Datenbanken abgecheckt, Patientenakten verwaltet, elektronische Arztbriefe ausgetauscht, Behandlungsdaten für Notfälle bereit gehalten und natürlich vor allem Gesundheitskosten automatisiert abgerechnet werden. Damit nicht genug der **Komplexität**. Derzeit sind in Deutschland mehr als 180 unterschiedliche Praxiscomputersysteme und mehr als 60 Klinik-Informationssysteme im Einsatz, für die nunmehr einheitliche Schnittstellen für perspektivisch alle soeben genannten Funktionalitäten geschaffen werden müssen.

In diesem Kontext kommt dem **Informationstechniker** bei der Gestaltung der elektronischen Gesundheitskarte eine **Verantwortung** zu, derer er sich wohl oft nicht bewusst ist. Die technische Gestaltung ist der Schlüssel für einen gerechten ökonomischen Interessenausgleich und zugleich der Schlüssel zur Wahrung von Vertraulichkeit und Wahlfreiheit bei Arzt und Patient. Es geht also nicht nur darum, eine fehlerfrei arbeitende Infrastruktur aufzubauen und Chipkarten, Lesegeräte, Praxissysteme und Netze mit einer funktionstüchtigen Hard- und Software auszustatten. Es geht auch darum, das Arzt-Patienten-Verhältnis zu schützen. Spätestens seit Galilei gibt es Wissenschaftler, die sich ihrer gesellschaftlichen Verantwortung bewusst sind. Seitdem gibt es aber auch solche, denen der schnelle Euro und die billige Lösung wichtiger sind. Und es gibt viele Einflüsterer, die sich gerne der Unterstützung der Techniker bedienen, um ihre ganz egoistische Interessen umzusetzen.

Das Projekt der elektronischen Gesundheitskarte ist somit nicht nur ein technisch ambitioniertes IT-Projekt, es ist vielmehr auch ein mindestens ebenso **ambitioniertes gesellschaftspolitisches Projekt**, das Gesundheitspolitiker, Patientenvertreter, Datenschützer, Ärztevertreter und

Medizinproduktevertreter dazu zwingt sich mit technischen Details auseinanderzusetzen. Dieses Projekt zwingt zugleich die Informatiker, sich mit den sozialen Rahmenbedingungen und Konsequenzen ihrer technischen Lösungen zu beschäftigen. Diesen werden Gewissensfragen gestellt. Sie bekommen eine gesellschaftliche Aufgabe, bei der er sie Partei für den kranken Patienten ergreifen müssen als indirekter, verlängerter Arm oder Gehilfe der Ärzte. Die Fragen, die die Informatiker vor ihrem Gewissen, ihren Arbeitgebern und ihren Technikerkollegen beanworten müssen, sind z.B. folgende:

- Genügen die vorgesehenen Datensätze den Prinzipien der Erforderlichkeit und der Datensparsamkeit?
- Sind die Daten während der Speicherung und bei Übermittlungen vor unberechtigtem Zugriff ausreichend geschützt, z.B. durch Verschlüsselung oder Pseudonymisierung?
- Ist durch das Zugriffskonzept gewährleistet, dass die Lese- und Schreibberechtigungen jeweils nur im Rahmen des Erforderlichen bzw. des vom Patienten Zugelassenen eingeräumt werden, z.B. durch Rollenkonzepte und hierarchische Zuordnungen?
- Ist gewährleistet, dass der Urheber jedes Datums eindeutig identifiziert werden kann, dass Nutzungen vollständig protokolliert werden?
- Sind die Daten so abgelegt, dass bei einer externen Systemadministration kein Einblick in patientenbezogene Daten möglich ist, z.B. durch eine pseudonyme oder verschlüsselte Ablage?
- Wird der mindestens 10jährigen Dokumentationspflicht genügt?
- Ist es dennoch möglich, den rechtlichen Anforderungen zur Löschung und Sperrung von Daten zu genügen?
- Ist eine umfassende Auskunftserteilung an den Patienten technisch problemlos möglich?
- Sind die Wahlrechte der Patienten auch tatsächlich technisch abgebildet?
- Ist die Anwender- und die Patientenoberfläche so gestaltet, dass Ärzte und Behandelte eine weitgehende Kontrolle über die Abläufe erhalten?
- Ist die Handhabbarkeit auch für Alte und Behinderte oder für Menschen ohne Computererfahrung gesichert?

VI. Konsequenzen für eine patientenfreundliche Implementation

Es wäre unfair, die Informatiker mit diesen Fragen alleine zu lassen. Diese haben - wie am Beispiel der elektronischen Gesundheitskarte mehr als deutlich wird - als wichtige Mitgestalter unserer Informationsgesellschaft eine zentrale kultur- und sozialpolitische Aufgabe. Damit sie dieser Verantwortung gerecht werden können, müssen ihnen die nötigen Rahmenbedingungen geschaffen werden. Diese Rahmenbedingungen werden nicht von den Technikern gesetzt, sondern von den **Unternehmen und Stellen**, für die die Informatiker tätig sind. Es geht also um die Vorgaben durch die Ministerien, die Krankenkassen, die Softwarehäuser, die medizinischen Berufsverbände, die Datenschützer. All diese Stellen sind mit verantwortlich, dass letztendlich die Techniker gute Arbeit leisten können. Dabei sind überzogene Wunschkataloge hinsichtlich Funktionalitäten oder Geschwindigkeit bei der Lösung eines technischen Problems Gift. Das Scheitern vieler Großprojekte, angefangen von TollCollect über den ersten Versuch der Installation von INPOL-Neu, über viele versandete E-Government- und E-Health-Projekte bis hin zum aktuellen Kontoevidenzverfahren im Finanzbereich legt es nahe, bestimmte Rahmenbedingungen zu beachten, die für eine vertrauenswürdige Technikgestaltung und damit für die Einführung der elektronischen Gesundheitskarte dringend geboten sind.

Ich möchte auf **vier Rahmenbedingungen** eingehen:

- das Erfordernis eines modularen Entwicklungsprozesses,
- die Transparenz des Verfahrens,

- die unabhängige Auditierung und die
- einführungsbegleitende Vermittlung von Medienkompetenz.

Unsinnig ist die Erwartung, ein komplexes Verfahren wie das der elektronischen Gesundheitskarte mit einem Schlag einzuführen. Hierbei kann es sich nur um einen vielstufigen Prozess, bei dem auf jeder Stufe zunächst eine Stabilität erreicht werden muss, um die nächste Stufe angehen zu können. Dieses Stabilität betrifft nicht nur den rein technischen Bereich. Vielmehr müssen auch die sog. "weichen Faktoren" berücksichtigt werden. Die Anwendenden und die Betroffenen sind auf jede Stufe vorzubereiten und zu begleiten. Bei dem **modularen Vorgehen** sind zunächst die Basisanwendungen zu implementieren. Bei der elektronischen Gesundheitskarte sind dies die schon bisher genutzte Abrechnungsfunktion, die Ausweitung der Identifizierungsfunktionen der Karte und als grundlegende Datentransportanwendung im Massenverfahren das elektronische Rezept. Diese Herangehensweise ist im Gesetz angelegt. Dem flächendeckenden Verfahren sind Erprobungen in Pilotregionen vorzuschalten, bei denen teilweise unterschiedliche Lösungen getestet werden und die skuzessive zusammenwachsen.

In jeder Entwicklungsstufe bedarf es eines Evaluierungsprozesses, in den möglichst sämtliche Betroffenen einbezogen werden sollten. Dies wiederum bedingt weitestgehende **Transparenz** des gesamten Entscheidungs- und Implementierungsverfahrens. Ohne die Möglichkeit der Hinterfragung jedes Bausteins des Gesamtverfahrens liefe man Gefahr, dass einer dieser Bausteine brüchig wird und das Gesamtprojekt zum Absturz bringt. Das Transparenzerfordernis gilt sowohl für die normative wie für die technische Seite, d.h. für die inhaltlichen Festlegungen von Datenfeldern, Sicherheitsanforderungen und Kommunikationsstandards wie für deren technische Definition und Umsetzung. Dabei ist Quantität nicht gleich Qualität. So konnte ich feststellen, dass in der Vergangenheit teilweise dicke Anforderungskataloge zur elektronischen Gesundheitskarte produziert wurden, deren Aussagekraft - freundlich gesagt - bescheiden waren.

Sicherheit lässt sich nicht im Dunkeln realisieren, schon gar nicht bei einem derart komplexen Verfahren mit derart vielen Beteiligten. **Security by obscurity** würde bei einem Projekt wie der elektronischen Gesundheitskarte fast zwangsläufig zum Scheitern führen. Dabei kann das Transparenzerfordernis bis in die Quellcode-Ebene reichen. Erlauben Sie mir insofern eine kritische Randbemerkung: Transparenz bedingt auch Pluralität. Monopolisierungsbestrebungen bestimmter Software-Anbieter durch den Versuch, eigene Standards zu allgemeinen Standards zu erheben, sind für das Gesamtprojekt schädlich und schaden letztendlich auch denen, die diese Bestrebungen verfolgen. Insofern empfinde ich die Erfahrungen mit dem Pilotprojekt Gesundheitskarte Schleswig-Holstein äußerst erfreulich, wo sämtliche Beteiligten an einem runden Tisch sitzen, ihre Vorstellungen ausdiskutieren und die Konsenssuche im Vordergrund steht.

Kaum berücksichtigt wurde bisher die Notwendigkeit einer **unabhängigen Auditierung**. Hierfür gibt es bisher kaum vorgegebene Instrumentarien. Ein Aspekt ist der Einsatz zertifizierter Einzelprodukte in dem erheblich umfangreicheren Telematik-Gesamtverfahren; ein weiterer Aspekt liegt in der Gesamtauditierung von größeren separierbaren Verfahrensteilen bzw. Modulen. Bei der Auditierung darf man sich nicht auf die technische Basis beschränken. Auditiert werden müssen im Grunde sowohl die organistorischen Vorgaben, als auch die Beachtung der rechtlichen Vorfestlegungen sowie die konkreten technischen Umsetzungsschritte.

Im Datenschutzrecht kennen wir eine Miniaturlösung eines Audits in Form der sog. Vorabkontrolle, die vom jeweiligen betrieblichen oder behördlichen Datenschutzbeauftragten durchgeführt werden soll. Schon einzelne Module der elektronischen Gesundheitskarte können aber die Möglichkeiten eines einzelnen Datenschutzbeauftragten überfordern. Daher wurden in Schleswig-Holstein als Ergänzung auf freiwilliger Ebene Verfahren zur Auditierung **von IT-Produkten sowie von Gesamtverfahren** eingeführt. Die Ergebnisse dieser Auditierungsprozesses, an dem grundsätzlich Gutachter und eine staatliche Zertifizierungsinstanz beteiligt sind, werden veröffentlicht. Hierdurch wird der Auditierungsprozess nachvollzieh- und hinterfragbar. Dies wiederum ist die Grundlage des Vertrauens insbesondere für die technikferneren Beteiligten, also hier Ärzte- und Patientenschaft sowie die allgemeine Öffentlichkeit. Die Verleihung des Audits muss durch eine vertrauenswürdige,

daher unabhängige Instanz erfolgen, um schon im Vorfeld dem Vorwurf der Parteilichkeit und mangelnden Objektivität entgegentreten zu können.

Auf **Bundesebene** gibt es zwar seit dem Jahr 2001 die gesetzliche Absichtserklärung, Auditverfahren einzuführen. Zu meiner großen Verwunderung hat aber bisher das insofern verantwortliche Innenministerium bisher auch nicht ansatzweise den Versuch unternommen, dieser Ankündigung weitere Schritte folgen zu lassen. Ganz anders in **Schleswig-Holstein**, wo seit über 4 Jahren erfolgreich Audit- und Gütesiegelverfahren durchgeführt werden. Viele Unternehmen wie auch die Verwaltung selbst haben erkannt, dass die Akzeptanz von IT-Systemen ebenso wie deren Qualität davon abhängt, dass sie einem unabhängigen Evaluierungsprozess unterzogen wurden. Ich habe die Hoffnung, dass die Win-Win-Erfahrungen in Schleswig-Holstein auch auf Bundesebene bald dazu führen, dass vergleichbare Verfahren eingeführt werden. Die damit verbundenen Kosten sind minimal im Vergleich zu den zu erzielenden Gewinnen. Schon heute ist das Unabhängige Landeszentrum für Datenschutz bereit, im Rahmen seiner Zuständigkeit Module der elektronischen Gesundheitskarte zu auditieren.

Gerade im **Medizinbereich** allgemein und bei der elektronischen Gesundheitskarte speziell zeigt sich die Sinnhaftigkeit von Auditierungsverfahren. Allein die Behauptung, Wahlfreiheit und Patientengeheimnis würden berücksichtigt, wird in der Bevölkerung keinen Glauben finden, insbesondere wenn diese Behauptung von interessierter Seite aufgestellt wird. Vertrauen findet allenfalls das unabhängige Votum einer vertrauenswürdigen Stelle.

Einem weiteren Aspekt wurde bisher bei der Einführung der elektronischen Gesundheitskarte eine viel zu geringe Aufmerksamkeit gewidmet: Ohne die Heranführung der Bevölkerung an dieses Medium wird dessen Einführung nicht gelingen. Die Vermittlung von **Medienkompetenz** betrifft zunächst die Patientinnen und Patienten. Diese müssen mit der Karte und den einzelnen Anwendungen vertraut gemacht werden. Dies geht nur bedächtig und fortschreitend. Die Vermittlung der nötigen Patientenkompetenz ist auch nicht zum Nulltarif möglich. Mit Erschrecken muss ich immer wieder fest, dass bei der Kalkulation von IT-Projekten kaum ein Augenmerk gelegt wird auf die Kosten, die mit der Ausbildung der Anwendenden und der Vermittlung gegenüber den Betroffenen verbunden ist. Den Patienten müssen die Abläufe mit der Karte vertraut gemacht werden, ihnen muss eine Vorstellung von den ausgelösten elektronischen Kommunikationsbeziehungen vermittelt werden und sie müssen in die Lage gesetzt werden, ihr Selbstbestimmungsrecht durch Optionen und Auskunftserteilung praktisch zu realisieren. Nicht weniger einfach ist die Ausbildung der Menschen in den Heilberufen, die künftig nicht nur mit der Gesundheitskarte, sondern auch mit ihrer Signaturkarte und mit ihren proprietären Hintergrundsystemen umzugehen in der Lage sein müssen.

VII. Schlussfolgerungen

Ich werde immer wieder von Vertretern der Ärzteschaft, von Patienten und Journalisten gefragt: Entspricht die elektronische Gesundheitskarte dem Datenschutz? Ist die Vertraulichkeit der Arzt-Patienten-Beziehung gewährleistet? Meine Antwort ist dann: Im Prinzip ja. Ob ich dies aber noch in einem Jahr sagen werde, wenn die Karte zumindest in einzelnen Regionen engeführt sein soll, kann und will ich nicht vorhersagen. Die gesetzlichen Rahmenbedingungen sind ermutigend. Meine praktischen Erfahrungen in Schleswig-Holstein mit dem Gesundheitsnetzwerk in Flensburg sind es auch. Aber mir ist bewusst, dass noch viele Weichen gestellt werden müssen, bevor wir nach flächendeckender Etablierung einer E-Health-Telematik-Infrastruktur nicht nur ein funktionierendes, sondern auch ein sicheres System bekommen. Einen wichtigen Beitrag hierzu leistet die Sicherheitstechnik. Deshalb habe ich große **Erwartungen an die Informatiker**. Sie können die Vertraulichkeit im Gesundheitswesen aus der Zeit des Hippokrates in unser Informationszeitalter nicht allein hinüberretten. Aber ohne sie wäre Vertraulichkeit nichts mehr als eine leere Worthülse.

Die elektronische Gesundheitskarte bleibt eine gesellschaftliche und technische Herausforderung mit gewaltigen wirtschaftlichen Auswirkungen. Sie kann zum Musterbeispiel werden, wie durch **intelligente technische Gestaltung** technische Neuerungen etabliert werden, die nicht nur große finanzielle Einspareffekte zur Folge haben, sondern zugleich die Autonomie, die medizinische und

informationelle Selbstbestimmung der Betroffenen respektiert, ja evtl. sogar fördern. Bisweilen ist der Verdacht geäußert worden, das Projekt der elektronischen Gesundheitskarte sei ein gewaltiges Auftragsbeschaffungsprogramm der IT-Industrie. Dass es dies nicht ist, sondern ein Zukunftsprojekt im Interesse der Gesundheit der gesamten Bevölkerung, diesen Beleg müssen die Beteiligten erst noch liefern.

Ich habe ein wenig die Hoffnung, dass Politiker am Beispiel der elektronische Gesundheitskarte lernen, dass sie ihre IT-Visionen nicht gegen die Bevölkerung realisieren können und dürfen und dass eine unabdingbare Voraussetzung für die Weiterentwicklung unserer freiheitlichen und demokratischen Gesellschaft im Informationszeitalter die Respektierung der Selbstbestimmung der Menschen ist. Diese Lektion hat die Politik bei der elektronischen Gesundheitskarte - so ist mein Eindruck - bisher verstanden. Leider gibt es Dutzende von anderen Beispielen, die insofern von einem ganz anderen Denken der Entscheidungsträger zeugen. Ich wünsche mir, dass Technik, Politik und Bürger im Interesse des Gemeinwohls einen **gemeinsamen Weg in die Informationsgesellschaft** suchen. Die elektronische Gesundheitskarte könnte hierfür ein Pilotprojekt werden.