Markus Christen/Endre Bangerter

20 Informatisierung in der Medizin

Fallbeispiel

Der 60-jährige Herr X steht zur Wiederwahl als Stadtpräsident. Vor einigen Wochen besuchte er einen Neurologen, weil er das Gefühl hat, er vergesse wichtige Dinge. Dieser teilt ihm ein beunruhigendes Ergebnis mit: es finden sich Anzeichen einer demenziellen Erkrankung; Auswirkungen auf den Alltag sind aber nicht vor frühestens fünf Jahren zu erwarten, und Medikamente können das Voranschreiten der Krankheit verzögern. Der Neurologe speichert die Diagnose in das elektronischen Patientendossiers von Herrn X, damit dieser die Information für die Therapieplanung zur Hand hat. Herr X ist sich der Brisanz dieser Information angesichts des Wahlkampfes bewusst. Entsprechend sperrt er in seinem elektronischen Patientendossier seinen Ärzten das Einsichtsrecht in die Diagnose, er will erst nach seiner (erhofften) Wiederwahl das Thema angehen. Doch Herr X weiss nicht, dass sein Computer kürzlich gezielt angegriffen und mit einem Trojaner infiziert wurde. Der Trojaner speichert alle auf dem Bildschirm des befallenen Computers gezeigten Informationen und übermittelt diese dem Computer des Angreifers. Wenige Tage später erhält Herr X in offensichtlich erpresserischer Absicht eine anonyme E-Mail mit einem angehängten Screenshot der Demenz-Diagnose.

20.1 Problemfelder

Informations- und Kommunikationstechnologie (ICT) hat seit den 1970er Jahren unzählige Prozesse im Alltag der Menschen verändert – so auch in der Medizin (Levy 1977). Beispiele sind die Digitalisierung der Informationsflüsse (z. B. *electronic health records*; Häyrinen et al. 2008), drahtlos gesteuerte medizintechnische Systeme (z. B. Implantate, Carranza et al. 2011) oder die Nutzung „intelligenter" technischer Systeme (z. B. Roboter, Ponnusamy et al. 2011). Wir beschränken uns auf die sog. „*eHealth*". Diese beinhaltet (Black et al. 2011): 1) Technologien zur Speicherung, zum Umgang und zur Übertragung von Daten; 2) (Experten-)Systeme zur Unterstützung klinischer Entscheide; 3) Telemedizin. Unser Fallbeispiel gehört in den ersten Bereich. Der Umgang mit medizinischen Daten stellt dabei ethische Fragen, die über die herkömmliche Datenschutz-Diskussion hinausgehen und angesichts der umfangreichen Förderung von *eHealth* vermehrt Gewicht erhalten. Beispiele solcher Initiativen sind die *Strategie eHealth Schweiz* (www.e-health-suisse.ch), die (private) elektronische Gesundheitsakte für Patienten (z. B. www.gesundheitsakte.de) und die elektronische Fallakte für Ärzte (www.fallakte.de) in Deutschland sowie die nationale elektronische Gesundheitsakte (www.elga.gv.at) in Österreich. Auf EU-Ebene wird mit der Richtlinie 2011/24/EU über Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung die

Schaffung eines zentralen europäischen Gesundheitsakten-Systems noch vor dem Jahr 2020 angestrebt.

Solche Systeme bringen zwei Veränderungen mit sich: 1) Man kann ortsunabhängig auf medizinische Information zugreifen; 2) auch der Patient kann diese Information einsehen. So soll das elektronische Patientendossier in der Schweiz es jeder Person ermöglichen, bis zum Jahr 2015 den Fachleuten ihrer Wahl unabhängig von Ort und Zeit relevante medizinische Informationen über ihre Person zugänglich machen zu können. Diese Digitalisierung von Informationsprozessen ist mit folgenden Problemfeldern verbunden:

1. *Informationssicherheit*: Die Digitalisierung und Speicherung medizinischer Information soll es erlauben, dass für Diagnose und Therapie relevante Informationen einfach verfügbar sind und nicht verloren gehen. Dieses Ziel stellt automatisch die Folgefrage nach der Sicherung dieser Information vor unbefugtem Zugriff (Kierkegaard 2011).
2. *Informationsnutzung*: Die in medizinische Prozesse eingebundenen Beteiligten (Patient, Arzt, Spital, Versicherer, etc.) haben unterschiedliche Interessen an den digitalisierten Informationen. Dies stellt Fragen nach Zugriffsrechten, Anonymisierung etc.
3. *Informationsverzerrung*: Die Digitalisierung von Informationsflüssen geht mit Standardisierungen einher. Bei bestimmten technischen Umsetzungen kann dies dazu führen, dass Informationen verzerrend dargestellt werden.
4. *Aufwand-Ertrag-Abschätzung der Informatisierung*: Die Schaffung elektronischer Gesundheitsdienste ist ressourcenintensiv und mit hohen Erwartungen verbunden. Es stellt sich Frage, ob Aufwand und Ertrag den Erwartungen entsprechen.
5. *Nichtintendierte Effekte der Informatisierung*: Die Möglichkeiten, die elektronische Patientendossiers bieten, können unbeabsichtigte Nebeneffekte haben.

Diese Problemfelder werden nachfolgend in ethischer und rechtlicher Hinsicht diskutiert, wobei wir vor allem dem Punkt Informationssicherheit Gewicht geben.

20.2 Ethische Beurteilung

Die Digitalisierung medizinischer Informationen hat diverse Vorteile, die bei einer ethischen Beurteilung der Sachlage berücksichtigt werden müssen. Beispielsweise zeigen erste Erfahrungen im Rahmen von *eHealth Schweiz*, dass insbesondere chronisch Kranke die neuen Möglichkeiten elektronischer Patientenakten sehr schätzen (Holm J, persönliche Mitteilung vom 27. 07. 2012). Wir diskutieren nachfolgend im Sinne einer *worst-case*-Abschätzung Probleme, die die unterschiedlichen *eHealth*-Systeme mit sich bringen können.

Informationssicherheit

Unzweifelhaft haben Informationen über den Gesundheitsstatus von Personen einen hohen ethischen Schutzwert. Sie betreffen das Selbstverständnis einer Person, aber auch ihr sozialer Status hängt von solchen Informationen ab (z. B. bei einer Stellenbewerbung). Entsprechend unterliegen medizinische Informationen (z. B. Wissen über genetische Krankheitsdispositionen) in rechtlicher Hinsicht hohen Datenschutzanforderungen, die nur in Ausnahmefällen (z. B. bei Epidemien) übergangen werden dürfen. So ist unbestritten, dass dem Datenschutz und der Privacy (das Recht, dass eine Person die Verbreitung der sie betreffenden Information selbst kontrollieren darf) in ethischer Hinsicht eine zentrale Rolle zukommen. Die Digitalisierung medizinischer Information zwecks vereinfachter Verfügbarkeit erschwert aber den Datenschutz. Der Grund dafür ist bekannt: Man kann mit viel Aufwand zentrale Server sehr sicher machen, im Allgemeinen aber nicht die Rechner der Endnutzer (also Ärzte und Patienten). Der Grund hierfür ist, dass – angesichts der Vielzahl an Angriffs-Strategien mittels Schadsoftware (*malware*) – Computer von Endnutzern nicht ausreichend vor Datendiebstahl geschützt werden, da dies den Endnutzer technisch schlicht überfordert (Blunden 2012; Zeltser 2012).

Wie groß das Risiko eines Angriffs ist, hängt vom Wert der Information ab, bzw. dem Anreiz eines potenziellen Angreifers, sich dieser Information unbefugt zu bemächtigen. Die Gewährleistung von Sicherheit ergibt sich demnach als *trade-off* zwischen den Kosten für den Schutz der Information und den Kosten, die aus einem erfolgreichen Angriff resultieren. Entsprechend sind die Schutzvorrichtungen für zentrale Serversysteme sehr hoch – Bankenrechner beispielsweise gelten als praktisch unangreifbar, zumal ein erfolgreicher Angriff potenziell die Kontendaten tausender Kunden betreffen würde. Analog muss von den Servern für die elektronischen Patientendossiers ein vergleichbares Schutzniveau gefordert werden. Dies kann technisch (mit hohem Aufwand) erfüllt werden (siehe z. B. Agrawal und Johnson 2007). In dieser Hinsicht ergeben sich keine neuen Fragen, wenn medizinische Informationen digitalisiert werden.

Die Sachlage ändert sich, wenn es um den Endnutzer geht, wie der Vergleich zum Online Banking zeigt. Hier kommt es nicht selten zu erfolgreichen Angriffen auf Konten, die (in Abhängigkeit von der Rechtslage im jeweiligen Land) in der Regel diskret „korrigiert" werden, um das Vertrauen in das System und damit dessen Effizienz nicht zu schädigen (Moore und Anderson 2012). Die Vorteile des Systems (geringe Kosten von online-Transaktionen) überwiegen die Verluste durch kriminelle Angriffe. In ethischer Hinsicht relevant ist dabei insbesondere, dass man bei solchen Angriffen den Schaden rückgängig machen kann. Im Fall von Gesundheitsinformationen greift dieses Argument aber nicht mehr, wie das Fallbeispiel verdeutlicht. Relevant ist hier die Information selbst (z. B. Erpressungswert des Wissens über eine Krankheit) und nicht, was damit gemacht werden kann (z. B. Konto plündern). Angriffe auf *eHealth*-Daten mögen derzeit zwar noch hypothetisch sein, Angriffe auf Kontodaten und Kreditkarteninformationen sowie „Identitätsdiebstahl" bilden derzeit noch den Regelfall. Doch die Erfahrung zeigt, dass Kriminelle rasch neue Betätigungsfelder finden.

Aktuell sind Angriffe mit sog. Ransomware, Schadsoftware, welche zu erpresserischen Zwecken den Computer sperrt. Dabei erscheint ein Fenster mit einer scheinbar offiziellen Nachricht, in der der Computerbenutzer aufgefordert wird, Bußgelder zu bezahlen, da sich auf seinem Computer illegales Material befinde (Melani 2011). Angesichts des hohen erpresserischen Wertes von Gesundheitsinformationen sind analoge Angriffs-Szenarien denkbar.

Kurz anzusprechen ist auch das Risiko der Manipulation von Information durch Angriffe auf Computer von Nutzern mit Schreibrechten für Daten (also z. B. bei elektronischen Patientendossiers der Computer des Arztes). Ein solcher Fall ist denkbar, aber unwahrscheinlicher, weil der Angriff komplizierter (man muss z. B. herausfinden, welchen Arzt ein bestimmter Patient hat) und der Erfolg unsicherer ist.

Informationsnutzung

Die in medizinische Prozesse eingebundenen Beteiligten haben unterschiedliche Interessen an digital erfassten Gesundheitsinformationen: Der Arzt will Informationen, die präzise den medizinischen Sachverhalt darlegen, um darauf gestützt Entscheidungen über Diagnose und Therapie fällen zu können. Das Spital benötigt Informationen für Planungs- und Budgetierungsentscheidungen und zur Rechtfertigung der eigenen Tätigkeit gegenüber z. B. politischen Instanzen. Krankenversicherungen wollen Informationen, für längerfristige Planungen (z. B. Prämienbestimmung) – aber auch zur gezielten Suche kostengünstiger Patienten. Der Patient schließlich wünscht verständliche Informationen. Diese unterschiedlichen Ansprüche gehen mit jeweils spezifischen Erfordernissen einher: So muss beispielsweise die Information für den Arzt klar einer Person zugeordnet sein, während Informationen für statistische Auswertungen durch Spitäler oder Versicherungen anonymisiert sind.

Diesen Erfordernissen trägt man dadurch Rechnung, indem Datenerhebung und -speicherung durch unterschiedliche Kanäle geschehen. Der zunehmende Druck z. B. aus Effizienzgründen entsprechende Informationskanäle und Datenbanken zusammenzulegen, kann aber diese Grenzen verwischen. Die ethische Forderung besteht hier darin, dass durch geeignete technische Maßnahmen solche „Grenzüberschreitungen" weitgehend ausgeschlossen werden können, d. h. Daten und Identifikationsmerkmale getrennt und unterschiedliche Pseudonyme für unterschiedliche Datenbanken verwendet werden.

Informationsverzerrung

Ziel der Digitalisierung von Informationsflüssen ist es, medizinische Informationen möglichst einfach zugänglich zu machen, was unzweifelhaft ein Vorteil ist und nachweislich Fehler z. B. durch nicht lesbare Handschriften reduziert. Paradoxerweise kann dies aber eine Verzerrung von Information zur Folge haben. Im Fall der *electronic health records* in den USA sind solche Effekte diskutiert worden (Greenhalgh et al. 2009), was zum einen mit der konkreten Art der Ausgestaltung der Eingabe-

Templates zu tun hat, zum anderen aber auch mit der veränderten Praxis der Abspeicherung von Information (z. B. standardisierte Eingabeboxen anstelle von handschriftlichen Notizen). Solche Zusammenhänge zwischen Medium und Botschaft wurden ausführlich im Rahmen der Toronto School of Communication Theory diskutiert (Watson und Blondheim 2008).

In ethischer Hinsicht ist klar, dass Verzerrung diagnose- und therapierelevanter Information vermieden werden muss. Entsprechend ist die technische Ausgestaltung so zu wählen, dass möglichst viel Information Template-Ungebunden (Freitextfeld) eingegeben werden kann. Dem wird beispielsweise bei den elektronischen Patientendossiers in der Schweiz Rechnung getragen – zweifellos ein Vorteil im Vergleich zu den stärker standardisierten Verfahren in den USA. Da aber Digitalisierung von Informationsflüssen dennoch einen Standardisierungseffekt hat, ist in ethischer Hinsicht zu fordern, dass digitalisierte Gesundheitsinformationen nicht zu einer generellen „Automatisierung" von medizinischen Prozessen führen dürfen. Der direkte Kontakt Arzt-Patient muss im Zentrum sein und entsprechende zeitliche Ressourcen müssen dafür reserviert werden.

Aufwand und Ertrag der Informatisierung

Die Digitalisierung der Informationsflüsse in der Medizin wird begleitet von Effizienzversprechungen, die angesichts der milliardenschweren Investitionen – England beispielsweise investierte jüngst 12.7 Milliarden Pfund in ein *National Programme for Information Technology* für den *National Health Service* (Greenhalgh et al. 2011), die US-Regierung stellte für ein vergleichbares Projekt 38 Milliarden US-Dollar zur Verfügung (Catwell und Sheikh 2009) – nicht verwundern. Allerdings ist trotz einer beachtlichen Literatur, welche den Effekt solcher Interventionen untersucht, die empirische Evidenz für positive Effekte erstaunlich gering (Black et al. 2011) und der Zeithorizont für eine Amortisierung der Investition wird auf 10 Jahre und mehr veranschlagt (Shekelle et al. 2006). Dies stellt die sozialethische Frage nach der Begründung solcher Investitionen angesichts der bekannten Finanzierungsprobleme des Gesundheitswesens. Eine solche Aufwand-Ertrag-Analyse sollte sich dabei nicht nur auf die Anfangsinvestition beschränken, sondern auch Effekte auf den Berufsalltag der Beteiligten beachten. Die oft beklagte „Bürokratisierung" des Arbeitsalltags in der Klinik kann gewiss nicht nur auf die Digitalisierung der Informationsflüsse zurückgeführt werden. Dennoch zeigen Untersuchungen praktische Schwierigkeiten, die in der Umsetzung großer *eHealth*-Initiative verbunden sind (z. B. Greenhalgh et al. 2011).

Nichtintendierte Effekte der Informatisierung

Eingriffe in die Abläufe des medizinischen Handelns – und die Digitalisierung der Informationsflüsse ist ein solcher Eingriff – können nichtintendierte Nebeneffekte haben. Beispielsweise kann die Verfügbarkeit medizinischer Information Einfluss auf Vertrauensverhältnisse des Patienten mit Dritten haben, weil damit ein sozialer Druck

zur Offenlegung verbunden sein kann. Wie genau mit solchen Situationen umzugehen ist, kann derzeit nur schwer beurteilt werden. Doch die Digitalisierung medizinischer Information – und damit auch die Explizierung der Informationsflüsse – dürfte das Vertrauen zwischen Personen, die in medizinische Prozesse eingebunden sind (Arzt-Patient, Arzt-Spitalmanagement, etc.), beeinflussen – positiv, aber eventuell auch negativ, denn Vertrauen drückt sich gerade in der Medizin dadurch aus, dass auf verantwortliche Weise mit sensibler Information umgegangen wird.

Ethische Empfehlungen

Im Licht obiger Erörterungen ergeben sich für das Fallbeispiele folgende konkrete Empfehlungen:

- Sorgfaltspflichten: Werden Dienstleistungen der eHealth genutzt, so müssen die beteiligten Endnutzer – also insbesondere Ärzte und Patienten – sich der „elektronischen Risiken" bewusst sein und bestehende Schutzmöglichkeiten müssen konsequent genutzt werden. So sollten beispielsweise Computer in Arztpraxen nicht für das „surfen" auf dem Internet genutzt werden, um Infektionen des Rechners mit malware zu vermeiden.
- Informationspflicht: Bei Dienstleistungen wie dem elektronischen Patientendossier muss vonseiten der Anbieter klar kommuniziert werden, dass diese Information nicht umfassend geschützt werden kann. Der Wunsch nach Effizienzsteigerung muss zurücktreten, d. h. man muss in Kauf nehmen, dass durch die Kommunikation der Sicherheitsproblematik weniger Personen das System nutzen.

Generell muss die Thematik Informationssicherheit und Privacy im Kontext der Medizin in der medizinethischen Debatte an Gewicht gewinnen, denn angesichts der enormen Möglichkeiten im *data mining*, sie sich durch die deutlich gewachsene Verfügbarkeit elektronischer Informationen sowie des veränderten Nutzerverhalten (z. B. soziale Netzwerke, in denen Patienten persönliche medizinische Informationen ablegen) ergeben, wird der Schutz dieser Werte in der Informationsgesellschaft zu einer zentralen Herausforderung (Van den Hoven et al. 2012; Vayena et al. 2012).

Literatur und Materialien

Agrawal R, Johnson C (2007) Securing electronic health records without impeding the flow of information. Intern J Med Inform 76:471–479

Black AD, Car J, Pagliari C, Anandan C, Cresswell K, Bokun T et al. (2011) The Impact of eHealth on the Quality and Safety of Health Care: A Systematic Overview. PLoS Med 8(1):e1000387

Blunden B (2012) The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, 2. Aufl. Jones & Bartlett, Burlington

Carranza N, Febles V, Hernández JA, Bardasano JL, Monteagudo JL et al. (2011) Patient safety and electromagnetic protection: a review. Health Phys 100(5):530–541

Catwell L, Sheikh A (2009) Evaluating eHealth interventions. PLoS Med 6:e1000126

Greenhalgh T, Potts HWW, Wong G, Bark P, Swinglehurst D (2009) Tensions and Paradoxes in Electronic Patient Record Research: A Systematic Literature Review Using the Meta-narrative Method. Milbank Q 87(4):729 – 788

Greenhalgh T, Russell J, Ashcroft RE, Parsons W. Why National eHealth Programs Need Dead Philosophers: Wittgensteinian Reflections on Policymakers' Reluctance to Learn from History. Milbank Q 89(4):533 – 563

Häyrinen K, Saranto K, Nykänen P (2008) Definition, structure, content, use and impacts of electronic health records: a review of the research literature. Intern J Med Inf 77(5):291 – 304

Kierkegaard P (2011) Electronic health record: Wiring Europe's healthcare. Comp Law Secur Rev 27, S. 503 – 515

Levy AH (1977) Is informatics a basic medical science? In: Shires DB, Wolf H (Hrsg.) Proceedings of the Second World Conference on Medical Informatics. Toronto, August 18 – 22. IFIP World Conf Ser Med Inf: 979 – 981

Melani (2011) Halbjahresbericht 2011/2. Melde- und Analysestelle Informationssicherung. http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de. Zugegriffen: 5. Sept. 2013

Moore T, Anderson R (2012) Internet Security. In: Peitz M, Waldfogel J (Hrsg.) The Oxford Handbook of the Digital Economy. Oxford University Press, Oxford

Ponnusamy K, Mohr C, Curet MJ (2011) Clinical outcomes with robotic surgery. Current Problems in Surger 48(9):577 – 656

Shekelle PG, Morton SC, Keeler EB (2006) Costs and benefits of health information technology. Evidence Reports / Technology Assessments 132. http://www.ncbi.nlm.nih.gov/books/NBK37988. Zugegriffen: 5. Sept. 2013

Van den Hoven J, Helbing D, Pedreschi D, Domingo-Ferrer J, Gianotti F, Christen M (2012) FuturICT – The Road towards Ethical ICT. European Physical Journal – Special Topics 214:153 – 181

Vayena E, Mastroianni A, Kahn J (2012) Ethical Issues in Health Research With Novel Online Sources. Am J Publ Health 102(12):2225 – 2230

Watson R, Blondheim M (Hrsg.) The Toronto School of Communication Theory: Interpretations, Extensions, Applications. The Hebrew University Magnes Press, Jerusalem

Zeltser L (2012) Understanding Modern Computer Attack and Defense Techniques. http://zeltser.com/computer-attacks-defenses. Zugegriffen: 5. Sept. 2013